Quizlet

CISSP Chapter 1

Study online at quizlet.com/_2eioym

1. **Describe the different levels of an organization and how security is implemented by them.**

   Senior management initiates and defines security policies.

   Middle management fleshes out standards, baselines, guidelines, and procedures.

   Operational managers and security professionals implement the controls.

   End users comply with it all.

2. **How can acquisitions and mergers pose security risks?**

   Data can be lost, co-mingled, or disclosed. In addition, downtime can occur that takes away from availability.

3. **How do the 3 points of the CIA triangle depend on each other?**

   Without confidentiality, you have no integrity. Without both, you cannot guarantee availability.

4. **In a business data classification scheme, what's the main difference between confidential and private data?**

   Both usually require the same security controls. However, confidential data usually has company information while private data is more individual information, like medical records.

5. **Should the different levels of documentation in a company be combined into one? Why?**

   No, the security policies, standards, baselines, guidelines, and procedures should be kept as separate entities. Not every user needs to know every single procedure. In addition, this makes it easier to enact changes.

6. **Should we layer controls in parallel or in series?**

   In series.

7. **What are the five elements of AAA services?**

   Identification
   Authentication
   Authorization
   Accounting
   Auditing

8. **What are the five government data classifications?**

   Top Secret
   Secret
   Confidential
   Sensitive
   Unclassified

9. **What are the five key concepts in reduction analysis or decompisition?**

   Trust Boundaries

   Data Flow Paths

   Input Points

   Privileged Operations (any activity requiring escalated privs)

   Details about security stance and approach

10. **What are the five principles COBIT has for governance and enterprise management?**

    1. Meeting stakeholder needs
    2. Covering the enterprise end to end
    3. Applying a single, integrated framework
    4. Enabling a holistic approach
    5. Separating governance from management

11. **What are the four business data classifications?**

    Confidential or Proprietary

    Private

    Sensitive

    Public

12. **What are the four levels of formal documentation for security in an organization? What does each discuss?**

    Policies - The scope of the security needed. Also used to assign roles, responsibilities, audit requirements. Explains why security is important in the company, and what assets are valuable. Defines acceptable risk.

    Standards - Define mandatory requirements for IT systems and homogenizes them. Baselines ensure all systems meet minimum security levels. Baselines may refer to standards like ITSEC, TCSEC, or NIST.

    Guidelines - Flexible. They recommend how standards and baselines should be implemented. These are not compulsory.

    Procedures - Detailed step by step instructions on how to implement security controls or solutions. If everyone follows the procedures, everyone will act securely.

13. **What are the seven steps to implement a classification scheme?**

Identify the custodian and his responsibilities.

Specify evaluation criteria.

Classify and label based on criteria.

Document exceptions to classification and integrate them into evaluation criteria.

Select security controls for each classification.

Specify prodedures to declassify or transferring custody to an external entity.

Create an organizational awareness plan and instruct all about the classification system.

14. **What are the six general security roles in an organization?**

Senior manager - signs off of security policies. Ultimately responsible.

Security Professional - Design and implement security solutions based on policies.

Data Owner - Classifies data and responsible for its protection.

Data Custodian - Follows data owner's policies and does actual testing and backing up of data.

User - Anyone using IT in the company. Restricted by principle of least privilege. Must understand security policies.

Auditor - Reviews policies and implementation, checks to see if they are being followed, produces compliance reports.

15. **What are the three overall categories of security policies?**

Advisory - Discusses behavior and activities that are acceptable. Defines consequences for violations. Explains senior management's desire for security and compliance.

Regulatory - Required when industry or legal standards apply to your company.

Informative - Provides information on company goals, mission statements, and provides background information relevant to specific pieces of the overall policy.

16. **What companies prioritize CIA points over other CIA points?**

Military and govt agencies tend to have confidentiality at the top. Private companies tend to have availability at the top.

17. **What does authorization look at?**

The permissions for the subject, object, and intended activity.

18. **What does every organization's security plan need?**

Approval and commitment by senior management. It's up to the policy development team to educate management on why it's needed.

19. **What initiates your accountability?**

Providing your identity. Computers track identities/user accounts, not subjects.

20. **What is abstraction?**

Grouping elements together into concepts. This allows us to assign permissions to groups more easily.

21. **What is a business case?**

A justification for a proposed project or undertaking.

22. **What is accountability dependent on?**

A strong authentication process. The reason is we must link the actions to a human. If authentication is weak, then we don't really know if the log on was legitimate.

23. **What is a parallel run?**

Change management test that tests functionality on a new and old system simultaneously to check if new system supports all required business functionality.

24. **What is architecture diagramming for?**

Lets you see, at a high level, how data flows between users, servers, and applications. Useful for mapping out how you want to protect that data.

25. **What is data concealment?**

Hiding data to prevent disclosure. Includes cover, obfuscation, and distraction. This is not the same as encryption.

26. **What is data privacy?**

Refers to keeping specific data (PII) confidential so as not to expose people and their information.

27. **What is data sensitivity?**

Refers to the quality of information, which could cause harm or damage if disclosed.

28. **What is reduction analysis?**

Decomposing an application, system, or environment for purposes of understanding its logic and how it interacts with external things.

29. **What is STRIDE? What does it stand for?**

A threat modeling guide that helps you categorize threats

Spoofing
Tampering (ruins integrity of info)
Repudiation (deleting evidence, blaming someone else)
Information Disclosure
Denial of Service
Escalation of Privilege

30. **What is the adversarial approach to threat modeling?**

Building, deploying, and then dealing with security issues. It's the whole point behind ethical hacking/penetration testing, source code review, etc.

31. **What is the defensive approach to threat modeling?**

Predicting threats and building into your code the defenses against them. Not all threats can be predicted though.

32. **What is the difference between auditing and accounting?**

Auditing records actions. Also called monitoring. Leaves proof for prosecution.

Accounting reviews those actions for compliance and violations to hold users accountable.

33. **What is the DREAD system?**

Used in threat modeling to help you decide on a level of risk.

Damage potential
Reproducibility (can the attackers do it over and over)
Exploitability (how hard is it to perform the attack)
Affected users
Discoverability (how hard is it to discover the weakness)

34. **What is the least secure authentication method?**

Passwords.

35. **What is the main goal of change management? What is its primary purpose?**

Ensuring changes to not lead to compromised security. Also offers rollback procedures. The primary purpose is to provide documentation for review and scrutiny by management.

36. **What is the purpose of data classification?**

Don't put too much effort into what doesn't need much protection and vice versa. Leads to efficiency. Can put data in groups for easy security controlling.

37. **What is threat modeling?**

Potential threats are identified, categorized, and analyzed.

38. **What might the analysis of a threat entail if the threat is a human and not a natural event?**

As an example, figure out what a hacker may want do to your website. His motives. Just disable it? Steal credit card info? Etc.

39. **What's are strategic, tactical, and operational plans?**

Long, medium, and short term plans. 5 years, 1 year, and day to day.

Strategic plans defines the organization's security purpose and aligns it to the company's goals. Updated yearly.

Tactical plans include projects, budgeting, and development plans. Can be ad hoc based on unexpected events.

Operational plans include scheduling, hiring, product designs, etc. Highly detailed.

40. **What should be identified in an architecture diagram?**

After the diagram is crafted, label the technologies including any OS, app, and protocols. Include version numbers and patches.

Then identify attacks that could happen to each target (all kinds, physical/social/technical/etc).

41. **What's the difference between due care and due diligence? Why are these important?**

Due care is using reasonable care to protect the interests of the company, while diligence are the activities practicing that care.

Management must perform due care/diligence to disprove negligence in case of a loss.

42. **Who does a security policy assign roles to?**

No individual in particular. The policy does not define who is to do what, but rather what must be done by various roles in the company.

43. **Who is security management a responsibility of?**

Upper management, not the IT staff. It is a business operations issue. The InfoSec teams should be autonomous.

44. **Why is change management important?**

Changes can introduce loopholes or oversights leading to new vulnerabilities or damage to CIA triangle.

Quizlet

CISSP Chapter 2

Study online at quizlet.com/_2ejhee

1.	**...**	...
2.	**How are AV, EF, and SLE related?**	AV * EF = SLE
3.	**How can you lower risks?**	Remove the threats or fix the vulnerabilities. Risk = threat * vulnerability
4.	**How does cross training differ from job rotation?**	Cross training means you are trained to do a co-worker's job in case they can't... however, you are not regularly rotated. It's just a back up plan.
5.	**How do NDAs and NCAs differ?**	NDAs stop you from giving away proprietary information. NCAs will stop you from jumping over to another company and having them benefit from your skills (usually there's a time frame on these).
6.	**In military and govt situations, what happens when you fail to meet requirements for third party governance?**	You lose your ATO (authorization to operate). To re-establish ATO, documents must be updated and an on-site review must show compliance.
7.	**In the realm of third party governance, what is documentation review?**	The exchange of documents between an organization and an auditor. The auditor verifies the organization against standards. If it holds up, than an on-site review will check for compliance.
8.	**Name different kinds of threats.**	Viruses, hurricanes, attackers, user ignorance, and power outage.
9.	**What are directive controls?**	These controls attempt to force or direct subjects to comply with something. Exit signs, posted notifications, and supervision.
10.	**What are some examples of administrative controls?**	Also known as management controls. Hiring procedures, background checks, exit interviews, vacation history.
11.	**What are some reasons you won't go with the best cost/benefit analysis?**	Budget limitations, favoritism, skills of IT staff, compatibility with current systems.
12.	**What are the six major steps in quantitative risk assessment?**	1. Inventory your assets and assign AVs. 2. List all threats of every asset. Assign asset EF and SLE. 3. Calculate ARO of each risk. 4. Calculate ALE. 5. Research countermeasures, and then recalculate ARO and ALE. 6. Perform cost/benefit analysis for each asset's threats.
13.	**What does EF stand for and what is it?**	Exposure Factor Percentage of AV lost experienced as a result of a realized risk.
14.	**What is a breach?**	When a threat agent bypasses or thwarts a security mechanism.
15.	**What is asset valuation?**	A dollar amount assigned to an asset based on actual costs, and non monetary expenses such as public confidence, industry support, knowledge benefit, etc.
16.	**What is exposure?**	The susceptibility of an asset to a threat.
17.	**What is hybrid analysis?**	Combining quantitative and qualitative risk assessments.
18.	**What is risk?**	The likelihood that a threat will exploit a vulnerability to cause damage to an asset.
19.	**What is risk analysis?**	The process of how you achieve the goals of risk management. Evaluate all risks on likelihood, damages, cost to mitigate, and present to upper management.
20.	**What is risk assignment?**	Same as risk transference.
21.	**What is risk rejection?**	Same as ignoring a risk.
22.	**What is security governance?**	Collections of practices related to supporting, defining, and directing the security efforts of an organization.
23.	**What is the delphi technique?**	An anonymous feedback-and-response technique where the cycle continues until a consensus is reached. It elicits honest and uninfluenced responses from everyone.
24.	**What is the primary goal of risk management?**	Reduce risk to an acceptable level depending on assets' value, budgets, organizational needs, practicality, etc.
25.	**What is the weakest element in any security solution?**	Humans.
26.	**What is total risk?**	Risk without any safeguards at all. threats + vulns + AVs = total risk

27. **What's the difference between awareness, training, and education?**

Awareness is just being aware. Training is being trained on how to comply with security standards. Education is going beyond what you need to know, usually for certifications or job promotions.

28. **What time of day and week should you terminate an employee?**

End of a shift so it's less stressful. Middle of the week so they have time to file for unemployment before the weekend.

29. **What two benefits does job rotation have?**

Knowledge redundancy - employees can take over for other employees. Less downtime this way. Keeps from getting more privileges at the same position over time.

Also acts as a check on someone else's work. Guards against fraud, collusion, sabotage, etc.

30. **What values do you need to calculate the cost/benefit analysis for risk management?**

ALE1 (original ALE)
ALE2 (safeguarded ALE)
ACS (annual cost of safeguards)

(ALE1 - ALE2) - ACS
Negative result means not worth it.

31. **When should you conduct an exit interview when terminating an employee? When do you remove his permissions? What do you do during an exit interview?**

Immediately upon termination. Restrict/remove his permissions during the exit interview. Review liabilities of the employee based on NDAs, NCAs, or any other agreements.

32. **Why is it important to maintain job descriptions even after positions have been filled?**

It will allow you to know somebody's responsibilities. They should regularly be reviewed. This will also ensure the principle of least privilege is still being applied, and avoid drifting.

33. **Why must security be measurable?**

To know if controls are providing a clear cost-benefit.

34. **Why should risk assessment be a continuous process?**

Security and risks change over time.

Quizlet

CISSP Chapter 3

Study online at quizlet.com/_2ek4j1

1. **Even if you dont have regulatory requirements for BCP (such as for banks, drug companies, or federal agencies), why might you still need to have BCP?**
You may be bounded by SLAs that you will not be able to satisfy. Thus, you will sever relationships with customers.

2. **How can you protect buildings and facilities?**
Use hardening provisions, or have an alternate site.

3. **What are SOC reports?**
Service Organization Control reports will ensure security controls are set into place for companies (like cloud providers) to show they can deliver on SLA targets in the event of disasters.

4. **What are the components of a BIA?**
ID priorities
ID risks
Likelihood and impact assessment
Resource prioritization

5. **What are the five steps to continuity planning?**
Strategy development
Provisions and processes
Plan approval
Plan implementation
Training and education

6. **What are the four main steps to BCP?**
Project scope and planning
Business impact assessment
Continuity planning
Approval and implementation

7. **What happens in the provisions and processes step of continuity planning?**
Design of the specific procedures that will mitigate the risks. The assets needed to be protected are people, facilities, and infrastructure.

8. **What happens in the strategy development step of continuity planning?**
The resource prioritization list produced in the BIA is looked over, and decisions made on which resources to protect and what risks are acceptable.

9. **What happens in the training and education step of continuity planning?**
BCP team members are trained, and back up members too. Everyone else in the organization is made aware of the plan.

10. **What is a business organizational analysis?**
This figures out who all the people are that would have a stake in BCP, such as core operational departments and also support structures like IT. It helps in choosing your BCP team.

11. **What is BCP?**
Business Continuity Planning identifies all risks to an organization's business processes, and then comes up with policies to minimize the impact of those risks to ensure continuity.

12. **What is continuity planning?**
This is done after the BIA. This will enact the procedures to ensure continuity.

13. **What is MTD/MTO**
Maximum Tolerable Downtime/Outage

The maximum time that a business process can be down without causing irreversible harm to the business.

14. **What is the BIA?**
The Business Impact Assessment will identify your critical resources, their threats, the likelihood of those threats attacking, and the impact of those attacks.

15. **What is the first task of BIA?**
Identify business priorities (also known as criticality prioritization) and rank them. This is qualitative. Then assign AVs to them. This is quantitative.

16. **What is the highest priority in BCP and DRP?**
People.

17. **What is the vital records program?**
This will be outlined in the BCP documentation. This document states where critical business records will be stored and the procedures for making and maintaining backups of those records.

18. **What should the relationship be between MTD and RTO?**
You want your RTO to be smaller than your MTD. This means you can recover operations before irreversible damage occurs.

19. **What's more important for the BIA, a quantitative or qualitative analysis?**
A balance of both is best.

20. **Whats the difference between BCP and DRP?**
BCP maintains critical business processes even if resources are strained. Once these processes become interrupted or stopped, then the DRP kicks in.

21. **What's the difference between RTO and RPO?**
Recovery Time Objective is how long it will take you to recover, where as the Recovery Point Objective is how much data going back you are prepared to lose.

22. **Which SOC reports are related to security and privacy?**	SOC-1 just covers internal financial reporting, so ask for the company's SOC-2 and SOC-3 reports.
23. **Who should be included in a BCP team?**	Someone from each department responsible for core services. Someone from senior management. IT people with technical skills applicable to BCP. Security personnel with BCP knowledge. Legal representatives who know corporate, regulatory, and contractual responsibilities.
24. **Who should perform the business organization analysis?**	Usually it's the spearheaders of the BCP team. But all members of the BCP team should review the analysis in case something was overlooked.

Quizlet

CISSP Chapter 4

Study online at quizlet.com/_2epmg
1

1. **How do you protect trade secrets?** If you copyright or patent them, the copyright will expire eventually. So you should implement controls in your company to protect them, like split knowledge and NDAs.

2. **What are the limits on using your own trademark?** They cannot be confusingly similar to another trademark. Have your lawyer do their due diligence on this. There will be an open opposition period where your trademark can be contested.

   It should not be descriptive of the goods and services that you offer. You cannot trademark "Mike's Software Company."

3. **What are the three criteria for a mission-critical system?** Defined as a national security system.

   Protected by procedures established for classified information.

   The security compromise of the information it processes would have large impact on the mission of an agency.

4. **What are the three main categories of law?** Criminal Law
   Civil Law
   Administrative Law

5. **What are the three main requirements of a patent?** Must be new, useful, and not obvious (using a cup to catch rain = rain catcher).

6. **What are the three provisions for the Federal Sentencing Guidelines?** Formalizing the prudent man rule, which requires senior executives to take responsibility for due care.

   Allowed lesser punishments for executives that can demonstrate due diligence in their information security.

   Outlined three proofs of negligence: The person accused must have a legally recognized obligation, he must have neglected them, and the failure must have directly led to the damages done.

7. **What did COPPA do?** Children Online Privacy Protetion Act of 1998 requires websites state what kind of information they collect, for what, and who its disclosed to. Parents must be provided with a shot to review this info, and give verifiable consent for anyone under age 13.

8. **What does CALEA do?** The Communications Assistance for Law Enforcement Act requires all communication carries to make wiretaps possible for law enforcement.

9. **What does copyright law protect in terms of software?** Only the original source code. It does not stop someone from rewriting it in a different form and accomplishing the same objective. You should treat your source code like a trade secret instead.

10. **What does DMCA do?** Digital Millenium Copyright Act punishes those who infringe on copyrights and circumvent their protections.

11. **What does FERPA do?** The Family Educational Rights and Privacy Act applies to educational facilities that accept government funding. It grants privacy rights to students over 18.

    Parents/students have the right to check their educational records maintained by the school, the request the correction of records and even a statement contesting uncorrected records, and schools cannot release personal information without consent.

12. **What does FISMA do?** The Federal Information Security Management Act rquires that federal agencies implement an information security program that cover the agency's operations. This includes the activity of their contractors.

13. **What does GISRA do?** Provides auditing authority to ensure all government agencies (even ones with non-classified info) implement controls to protect mission-critical systems.

14. **What does HIPAA do?** The Health Insurance Portability and Accountability ACt of 1996 requires health institutions to have strict security measures for hospitals, insurance companies, or anyone who stores or processes medical records.

    Also requires companies to disclose the individual's rights in writing.

15. **What does HITECH do?** Health Information Technology for Economic and Clinical Health Act of 2009 expands HIPAA to require breach notifications. Also, any business associates of a HIPAA compliant company must do their business in compliance as if they were a HIPAA company.

16. **What does the 1994 CFAA amendments do?** Expands CFAA to protect interstate commerce and not just federal or financial institutions, outlawed malicious code, can imprison offenders, and protects victims of computer crime by allowing them to sue for damages.

17. **What does the CCCA do?** The Comprehensive Crime Control Act was written to exclusively cover computer crimes that crossed state boundaries (so as not to infringe on states' rights). It also stopped access to classified or financial information on federal computers. In addition stopped tampering of any medical information.

18. **What does the CFAA do?**
The Computer Fraud and Abuse Act expanded the CFAA to include accessing anything at all unauthorized on any computer used exclusively by the US government or a financial institution. Punishes those that use computers in different states together to commit an offense.

19. **What does the Computer Security Act of 1987 do?**
This establishes baseline requirements for all federal computer systems. It gives NIST the responsibility for these standards and guidelines. This act also requires training for all people involved in using federal computers with sensitive information.

20. **What does the Electronic Communications Privacy Act of 1986 do?**
Makes it a crime to invade the electronic privacy of an individual.

21. **What does the EU Privacy Law require?**
Any organization processing personal data must meet one of the following: Consent, contract, legal obligation, vital interest of data subject, balance between interest of data holder and data subject.

The rights of the data subject are:
Right to access the data, its source, correct wrong data, withhold consent to have it processed in some situations, and legal action if these rights are violated.

22. **What does the Gramm-Leach-Bliley Act of 1999 do?**
There were strict government restrictions on what information can be passed between financial institutions. This law relaxes them a little, but requires private policies, enforces financial privacy, safeguards, and punishes using false pretext to access financial data.

23. **What does the Identity Theft and Assumption Deterrence Act do?**
Before, only the creditors of an ID theft victim were protected. Now the victims themselves are protected too and gives severe penalties for ID theft.

24. **What does the National Information Infrastructure Protection Act of 1996 do?**
Broadens CFAA to cover systems used in international commerce (not just interstate).

Extends coverage to national infrastructure like railraods, gas, pipelines, power grids, telecom circuits.

Treats intentional and reckless acts that cause damage to the above as a felony.

25. **What does the Uniform Computer Information Transactions Act enforce?**
Enforces shrink-wrap and click-through license agreements. Also requires an option to reject the terms and get a full refund.

26. **What does the USA PATRIOT Act of 2001 do?**
Broadened the government's powers to wiretap people, to obtain information from ISPs, and amends the CFAA to make more severe penalties for criminal acts.

27. **What do NIST and the NSA have authority over?**
NSA has authority over systems with classified information. NIST has authority over all other federal-use systems.

28. **What do the IS programs in FISMA require?**
Periodic risk assessments, policies and procedures based on them, security awareness training, periodic testing of controls, a process for planning implementing evaluating and documenting remedial actions to address deficiencies in the IS system, and incident response procedures.

29. **What is a patent?**
Protects the rights of an inventor to use and license the product.

30. **What is a trademark? What are they for?**
Words, slogans, and logos used to identify a company. They avoid confusion in the marketplace.

31. **What is a trade secret?**
Intellectual property that if disclosed will make you lose your business advantage. Like a secret formula.

32. **What is copyright law?**
Guarantees an original author protection against unauthorized copying of their work.

33. **What is the basis of privacy rights?**
The 4th Amendment.

34. **What is TM vs (R)?**
You get a TM as soon as you use a slogan. Just put TM on it. However, if you register it, you get the (R) symbol. You can register trademarks before you even use them this way. Also, they will check if it's been taken or not.

35. **What's the difference between criminal, civil, and administrative laws?**
Criminal laws can lead to imprisonment and fines.

In civil laws, only fines. The government just provides the judges, juries, and court and play an administrative role in managing the judicial system as according to the law.

Administrative laws are those that govern the daily activities of the agency. Like procedures and immigration policies.

36. **What two things did the Privacy Act of 1974 do?**	Agencies must maintain only personal records necessary for their business and destroy them when they are no long needed. Must provide individuals access to the records and correct them if needed.
37. **When do you get protected by copyright?**	You do not need to register for it to have it enforced. When you create it, you own it. Official registration is just official acknowledgement that it's your work.
38. **Which kinds of laws do not need approval from the legislative branch?**	The executive branch can make administrative laws as long as they comply with criminal and civil laws.
39. **Who owns a copyright?**	The owner of the work, unless it was a work for hire stipulated in a contract.

Quizlet

CISSP Chapter 5

Study online at quizlet.com/_2el514

1. **Explain cost center vs profit center.**

Security team is a cost center since they don't generate profits. Sales is a profit center.

The business side will sometimes view IT as reducing profits, so a healthy balance between the two is needed.

2. **How can you protect data in use?**

Data in use resides in an applications memory buffer. This buffer must be purged and completey removed from memory when the it's no longer needed.

3. **How do data classes map to govt and private company classification levels?**

Class 3 - Top Secret / Confidential
(Exceptionaly grave damage)

Class 2 - Secret / Private
(Serious damage)

Class 1 - Confidential / Sensitive
(Damage)

Class 0 - Unclassified / Public
(No damage)

4. **How does IPsec protect data?**

The AH provides authentication and integrity. The ESP provides confidentiality.

5. **What are some ways to digitally mark data?**

Change the metadata. This also allows DLP systems to detect it and ensure proper protection.

You can also put headers and footers on your documents. These will alsp show when printed.

6. **What are the four respnsibilities of a data owner according to NIST?**

Lay out the appropriate use and protection rules.

Advise info system owners on controls for the system where the data resides.

Decide who has access to the system and their permissions.

Help assess the system's security controls.

7. **What are the seven safe harbor principles?**

Notice - Tell the individuals the purpose of data collection.

Choice - Individuals can opt out.

Onward Transfer - The organization can only transfer data to other organization with notice and choice policies.

Security - Individual's data will be protected.

Data Integrity - Organizations can only use the data for the laid out purposes, and it must ensure the data is reliable.

Access - Individuals must have access to the data, and can delete/correct data when it is inaccurate.

Enforcement - Must implement mechanisms to ensure compliance with the principles.

8. **What does an asminislrator do?**

Grants permissions based on principle of least privilege and need to know. Usually uses RBAC by granting permissions to groups, and then assigning users to those groups.

9. **What do transport encryption methods do?**

Encrypt data before transmission happens.

10. **What five responsibilities does NIST lay out for system owners?**

Develop security plan for the system.

Maintain the plan and endure system is deployed in according to it.

Make sure users and support get proper training, like knowing rules of behavior or AUP.

Update the plan when changes occur.

Help assess and implement the systems security controls.

11. **What is a business/mission owner?**

They own a business process, like sales. They will use systems owned by a systems owner. They just ensure these systems provide value to the business processes.

12. **What is a data processor?**

A natural or legal person which processes personal data on behalf of the data controller who controls the data.

13. **What is a system owner?** Somebody who owns the information system where data resides. Usually this is the same person as the daya owner.

14. **What is record retention?** The act of retaining data for as long as it is needed, but destroying it when it is not.

15. **What is safe harbor's goal?** To follow principles that satisfy the EU Data Protection Directive. It prevents unauthorized disclosure of information handled by data processors, data controllers, and its transmission.

16. **What is sanitation?** The overall process that makes data completely unrecoverable by any means.

17. **What is the main reason data should be marked?** When users know the sensitivity of data, they are more likely to take appropriate steps to control and protect it properly.

18. **What level of protection should back ups of data have?** The same exact level as their originals.

19. **What media can be degaussed? What can't?** HDDs, magnetic tapes, and floppy drives can be degaussed.

CDs, DVDs, and SSDs can't be degaussed.

20. **What should you do if you want to downgrade a system or media to a lower classification level?** Sanitize it. Usually it's safer and cheaper to just destroy it and purchase new media instead of reusing it.

21. **What should you do when you no longer need sensitive data?** Destroy it.

22. **What's the difference between erasing, clearing, and purging?** Erasing just deletes.

Clearing will overwrite. This prepares the media for reuse. Sometimes a triple pass is used (bits, complements, random bits).

Purging is intended clearing of data involving degaussing and overwriting many times. Protects against any known recovery method. Still not good enough for US govt top secret data though.

23. **What's the difference between file level and disk level encryption?** One encrypts the entire disk. The other encrypts individual files.

24. **What transport encryption methods should be used when sending data internally?** IPsec and SSH. This allows for use of protocols like SFTP and SCP.

25. **Why can't you degauss SSDs?** They have circuitry instead of magnetic flix to store data so they don't have data remanence.

26. **Why isn't purging always trusted?** Bad sectors and SSDs can cause problems.

27. **Why should you also label data that is unclassified?** Removes ambiguity. If a user finds an unmarked folder that has confidential files, he won't automatically assume it's public so it will be handled with suspicion.

28. **Why should you still protect public or unclassified data?** You want to ensure its integrity. For example, you don't want attackers changing your welcome message.

Quizlet

CISSP Chapter 6

Study online at quizlet.com/_2epzm a

1. **Do secret keys give nonrepudiation?**

No. Only public/private key pairs can do that.

2. **How can you account for wrap around in a shift cipher?**

Use mod 26.

3. **How can you crack the Caesar cipher?**

Do a frequency analysis. For example, you know the letters E, T and A are very common. So whatever letter are common in the cipher text might correspond to E, T, and A.

4. **How should you protect secret keys?**

Never store it on the same system where the encrypted data resides. For sensitive keys, considering using split knowledge.

When a user who knows secret keys leaves an organization, you must replace all of the ones he knows and re-encrypt the information he can decrypt with the new keys.

5. **What are six strengths of public key cryptography? What's its weakness?**

Adding a user only adds a pair of public/private keys.

No preexisting communication link needs to exist. You can go straight ahead.

Key distribution is simple, if you want to join in just make your public key known. You can't derive the public key from the private key so this is safe.

Users can be removed easily. Just revoke their public key.

Key regeneration is only required if your private key is compromised.

It can provide nonrepudiation, integrity, and authentication.

However, it's a thousand times slower than a symmetric key!

6. **What are the five modes of operation for DES?!**

Electronic Code Book (ECB)
Just regular encryption on each block. That means a repeated block will have a repeated ciphertext. Weak! Only good for small amounts of data like keys and parameters, or cells in a database.

Cipher Block Chaining (CBC)
Random IV is XORed with the first block. Then encrypted. Then each successive block is XORed with the current block before being encrypted. Errors will propagate!

Cipher Feedback (CFB)
Just a stream cipher version of CBC, where it will put characters in a memory buffer until its a fit block size and then encrypt it. Errors propagate! IV and chaining is used.

Output Feedback (OFB)
Also a stream. IV is made to make a seed value. XOR with first block. Then encrypt the seed value to XOR it with the next block. Repeat. Errors do no propagate.

Counter (CTR)
A stream lIke CFB and OFB, but uses a counter which increments instead of seed values that need to keep getting encrypted. The counter is XORed with the block before it's encrypted.

7. **What are the four requirements of one time pads?**

The key must be as long as the plain text.
The key must be randomly generated.
The key must be used only once.
The key must be kept completely secret, so destroy it after use.

8. **What are the four things cryptographic systems hope to achieve?**

Confidentiality, integrity, authentication, nonrepudiation. Not all cryptosystems are designed to achieve all four though.

9. **What are the four weaknesses to symmetric key algorithms? What's its strength?**

Key distribution is difficult; if you can't use an a secure channel to do this, you need to do an out of band exchange.

They don't provide nonrepudiation.

The algorithm is not scalable since you need a symmetric key for every pair of people. Total keys is [n(n-1)]/2.

Keys must be regenerated often, especially when a participant leaves a group. Destroy all keys known by that participant.

However, it works a thousand times faster than public keys!

10. **What are the three main ways to exchange symmetric keys?**

Offline Distribution
Physical exchange. Can be on a sheet of paper or storage media. However, this can be intercepted.

Public Key Encryption
Encrypt it with someones public key, and that person can decrypt it with their private key. Requires a PKI.

Diffie-Hellman
An asymmetric key exchange algorithm useful for when there is no PKI.

11. **What are the two key escrow approaches?**

Fair Cryptosystem
Split up the keys into different pieces, and give them to independent third parties. A govt would need a court order to get them all together.

Escrowed Encryption Standard
Leave the key halves with the government, like in Skipjack.

12. **What does a substitution cipher do?**

Replaces letters or bits with others.

13. **What does a transposition cipher do?**

Rearranges letters around.

14. **What does Twofish do?**

A symmetric block cipher that supported pre and post whitening, which will XOR the plain text with a subkey before the first round of encrypting or after the final round of encrypting.

15. **What is 3Des? What are the different forms of it?**

3DES runs DES three times. It comes in different forms.
DES-EEE3: Encrypt K1, K2, K3 (168 bits)
DES-EEE2: Encrypt K1, K2, K1 (168 bits)
DES-EDE3: Encrypt K1, Decrypt K2, Encrypt K3 (112 bits)
DES-EDE2: Encrypt K1, Decrypt K2, Encrypt K1 (112 bits)

16. **What is a cryptosystem?**

Any implementation or technology involved in applying cryptographic algorithms.

17. **What is a key space?**

The range of values you can use as a key for an algorithm. Larger bit size = larger bit values. A 128 bit key has 2^128 values in its key space.

18. **What is a running key cipher?**

A book cipher. Make the key a sentence from a known book. This way you don't need a physical exchange of long, awkward keys.

19. **What is a Vernam cipher?**

A one time pad.

20. **What is a work function?**

Measures the strength of a cryptographic algorithm by computing how long a brute force attack would take against it.

21. **What is Blowfish?**

A block cipher that is faster than IDEA and DES.

22. **What is IDEA?**

International Data Encryption Algorithm.

23. **What is M of N control?**

This requires a minimum (M) number of agents (N) work together to complete a high-security task. Not just one person alone. It's part of the split knowledge mechanism.

24. **What is nonce?**

A random number that acts as a placeholder variable in a mathematical function. An IV is an example of a nonce.

25. **What is RC4 and RC5?**

RC4 is a stream cipher, RC5is a symmetric block cipher.

26. **What is Skipjack?**

Used by US government and has same five modes as DES. However, it supports key escrows with NIST and the Department of Treasury. To get the key you need to contact both agencies.

27. **What is split knowledge?**

Two different people knowing parts of the same thing. This is used in key escrows so that the key escrow administrator can't abuse his power.

28. **What is the biggest advantage of one time pads?**

There is no repeating pattern of alphabetic substitution so cryptoanalysis is useless.

29. **What is the Caesar cipher also known as?**

ROT3 cipher, if the shift is 3. Also known as a shift cipher.

30. **What is the difference between a code and a cipher?**

Codes are sometimes secret, but not necessarily to provide confidentiality. They replace words or phrases. They are just convenient.

Ciphers are always completely confidential and encrypt based on bits or characters.

31. **What is the difference between confusion and diffusion?**

Confusion is when the relationship between the plain text and cipher text is so confusing, that changing the plain text over and over to analyze the cipher text won't determine the key.

Diffusion just means a small change in the plain text will cause many changes in the cipher text.

32. **What is the Kerchoff Principle?**

The idea that a cryptographic system should be secure even if everything about the system (except the keys) is secure. "The enemy knows the system."

33. **What is zero knowledge proof?**

Proving to you I know something without giving it away. For example, I can prove to you I have your private key if I can decrypt a message encrypted with your public key and show the message to you.

34. **What kind of substitution protects against frequency analysis?**

Polyalphabetic (instead of monoalphabetic). However, it is still vulnerable to period analysis, which takes a closer look at repeated use of the key.

35. **What's another name for cryptographic keys?**

Cryptovariables.

36. **What's the difference between block and stream ciphers?**

Block ciphers operate on chunks at a time. Stream ciphers will operate on bits of characters at a time, like the Caesar Cipher or One Time Pad.

37. **What was DES superseded by?**

AES.

Quizlet

CISSP Chapter 7

Study online at quizlet.com/_2eqpq

1. **Can anyone set up shop as a CA?**
Sure, but who is going to trust you? The certificates issued by a CA are only as good as people trust them to be.

2. **Do digital signatures provide confidentiality?**
No. Only encrypting the message does that.

3. **How can you protect against undetected key compromise?**
Enact mandatory key rotation requirements.

4. **How does steganography work?**
You can hide data in plain sight by changing least significant bits so there's no noticeable difference.

5. **How do you digitally sign a message? How do you encrypt the whole message too?**
Write a message, then hash the message. Take the hash digest and encrypt it with your private key.

When the receiver gets the email, he will decrypt the encrypted hash digest with your public key, and then check the hash.

To encrypt the whole message, encrypt ALL of the above with the receivers public key first.

6. **How do you set up an IPsec session?**
You have to create a security association (SA) that represents a simplex connection. If you want a two way channel, you need two SAs. If you want AH and ESP both ways, then you need 4 SAs.

7. **How do you verify somebody's certificate?**
First check their certificate by using the CA's public key on it. Then make sure it has not been revoked (check a CRL or use OCSP). Then make sure the certificate contains the data you are actually trying to verify. And lastly... do you trust that CA in the first place?

8. **What are examples of link encryption and end to end encryption?**
IPsec in tunnel mode is end to end. So is IPsec/L2TP

SSH, SSL, and TLS are end to end encryption protocols.

9. **What are some examples of steganography?**
Adding a digital watermark to a piece of work. You can add unique ones so you can trace who shared your image.

10. **What are the five reasons your digital certificate can be invalid?**
It expired. Or, it was revoked because:
The private key was compromised
The CA erroneously issued it to you
The details of the certificate changed (like subject's name)
The security association changed

11. **What are the five requirements for a has function according to RSA Security?**
Input can be of any length,

but the output is always fixed.

The hash is easy to compute,

but nearly impossible to go backwards from.

The hash is collision-free.

12. **What are the four basic requirements of ISAKMP?**
Authenticate hte peers, create and manage the SA between them, provide the key generating mechanism, and then protect against threats.

13. **What are the steps to get your digital certificate?**
Fill out a CSR and prove your identity to the CA. Then give them your public key. They will create a certificate for you and sign it with their private key.

14. **What are the steps to SSL?**
When you go to a website, your browser takes that site's cert and extracts the public key.

Then your browser creates a symmetric key and encrypts it with the site's public key.

Then this symmetric key is safely sent to the site, so all communications are now symmetrically encrypted.

15. **What are two other names for a birthday attack?**
Collision attack or reverse hash matching.

16. **What are two ways to verify authentic, non-revoked certificates?**
Check a CRL. This has some latency between the revocation and when the CRL is updated though.

Another way is to use the online certificate status protocol. Use the OCSP with the certificate's serial number, and the server will repsond with valid, invalid, or unknown.

17. **What attack can defeat SSL?**
POODLE
Paddign Orcale n Downgraded Legacy Encryption

18. **What do digital signatures provide?**
Nonrepudiation, integrity, authentication.

19. **What do RAs do?**
Registration Authorities help CAs with the burden of identifying users' identities. They don't issue certificates themselves though. They allow CAs to remotely validate people.

20. **What information is on an X.509 digital certificate?**

Which version of X.509
Subject's name, public key, serial number of cert, and validity period.
CA name that issued it and their signature algorithm identifier.

21. **What is a chosen plaintext and chosen ciphertext attack?**

Chosen plaintext: you have the ability to encrypt some plaintexts and analyze what the key is.

Chosen ciphertext: you have the ability to decrypt some ciphertexts and analyze what the key is.

22. **What is a digital certificate?**

Basically just an endorsed copy of your public key. It's endorsed by a trusted CA (the CA signed it with their private key).

23. **What is a meet in the middle attack?**

This defeats two rounds of encryption. You take plaintext and encrypt it with every key, then you take cipher text and decrypt it with every key, and you look for matches.

24. **What is an analytic attack?**

An algebraic manipulation that tries to reduce the complexity of the algorithm. These attacks focus on the logic of the algorithm to attack it.

25. **What is an implementation attack?**

Focuses on exploiting a suboptimal implementation of an encryption algorithm.

26. **What is a statistical attack?**

This exploits statistical weaknesses in a cryptosystem, and its ability to truly create random numbers.

27. **What is El Gamal Encryption?**

It is an extension of the Diffie-Hellman Exchange. It was publicly released, unlike RSA at the time. It's disadvantage is that it doubles the length of any message it encrypts so it's bad for encrypting long messages.

28. **What is ISAKMP? What does it do?**

Internet Security Association and Key Management Protocol does the background work for IPsec to completely manage SAs.

29. **What is PGP?**

Pretty Good Privacy is used for digitally signing and encrypting emails. It combines the CA hierarchy of trust and makes a "web of trust."

The free version uses SHA-1 with CAST encryption and Diffie-Hellman for key exchange.
The commercial version uses MD5 with IDEA and RSA for key exchange.

30. **What is S/MIME?**

An email signing and encrypting standard. It relies on X.509 certificates. It supports RSA for key exchange, as well as AES and 3DES for encryption.

31. **What is the advantage of security associations (SAs) with IPsec?**

You can manage communication on a per-SA basis.

32. **What is the biggest flaw with DRM?**

You computer trying to access the encrypted movie must have the key stored on it too! So there's always a change you can manipulate your computer to get the key yourself.

33. **What is the goal of SSL?**

To create secure communication channels that remain open for the entire session.

34. **What is the known plaintext attack?**

You have a copy of the plain text and corresponding cipher text.

35. **What is X.509?**

Digital signatures can have different information on them. X.509 is just one standard that says what info will be on them.

36. **What kind of framework is IPsec?**

Open and modular. It does not dictate all implementation so many companies create different IPsec solutions.

37. **What kind of keys does IPsec use?**

It uses public keys to establish a secure connection to exchange a symmetric key.

38. **What's stronger, SHA-2 or MD5?**

Use SHA instead. MD5 isn't accepted by the US govt anymore, it still has hash collisions.

39. **What's the difference between IPsec's transport mode and tunnel mode?**

Tunnel mode encrypts the entire packet including headers and footers. Good for gateway to gateway communication.

Transport mode only encrypts the payload. Good for peer to peer communication.

40. **What's the difference between link encryption and end to end encryption?**

Link encryption encrypts the payload as well as headers and trailers. This means it's in a secure tunnel where each the packets must be decrypted at each hop, slowing it down.

End to end encryption only encrypts the payload, so you still can read the headers and trailers and know where the packet is going. This is faster.

41. **What's the major strength of public key cryptography, and what makes it possible?**

You can securely communicate with someone you've never met. This is possible due to the PKI.

42. **What two concepts do digital signatures rely on?**

Public key cryptography and hashes.

43. **Why is MD2 a weak hash?**	It's not a one way function.
44. **Why is MD4 a weak hash?**	Too many hash collisions. Modern PCs will find collisions in under a minute.
45. **Why should you use a key length longer than what you need now?**	Computing power increases very quickly. Encryption that takes 5 years to break today, may only take 1 year to break later.
46. **Why should you use HMACs at times, when they don't give nonrepudiation like digital signatures do?**	Since HMACs use symmetric keys, it's much faster. At times it will be enough to use an HMAC so you can benefit from its speed.

Quizlet

CISSP Chapter 8

Study online at quizlet.com/_2erlgv

1. **Explain security token vs capabilities list vs security label.**

   All 3 list the security attributes of the objects they refer to, but each has its own advantage. Tokens allow you to access the security list separately before you access the object. Capabilities list offer faster lookups. Security labels a part of the file itself, which gives anti-tampering control.

2. **How can you implement confinement?**

   Through the OS, through a confinement application, or through virtualization.

3. **What are functionality and assurance ratings?**

   Functionality ratings state how well the system does its functions it's supposed to. Assurance rating is the degree of confidence the system will work properly in a consistent manner.

4. **What are the bounds of a process?**

   The limits set on the memory addresses and resources it can access. You can also have physically (instead of logically) bounded processes on a different hardware. This is more expensive but more secure.

5. **What are the columns and rows of an access control matrix called?**

   Columns are ACLs, and rows are capability lists.

6. **What are the four categories for TCSEC's confidentiality ratings?**

   Category A - Verified protection.

   Category B - Mandatory protection.

   Category C - Discretionary protection.

   Category D - Minimal protection.

7. **What are the four rules in Take-Grant?**

   Take
   Grant
   Create
   Remove

8. **What does the simple security/integrity property do?**

   What about the * security/integrity?

   Simple is just where you can't read.

   Star is where you can't write.

9. **What do security models do?**

   Provide a formal way of creating security policies.

10. **What do TCSEC and ITSEC focus on differently?**

    TCSEC is all about confidentiality, while ITSEC is about all CIA.

11. **What is a constrained interface?**

    Think of fordham not having a volume button, or options being grayed out on your computer.

12. **What is a trusted computing base?**

    It's a theoretical small subcomponent of your computer that is completely secure, from which you will manage the rest of your computer. The security perimeter is the boundary to the rest of the computer and it communicates through trusted paths. It has a reference monitor that is an AC mechanism.

    The real life implementation of all this is called the security kernel.

13. **What is certification vs accreditation?**

    You certify a level of security for a system after evaluating it after reach change to its configuration. However, you accredit it for your company if you decide it meets your needs.

14. **What is confinement?**

    Allowing a process to read and write to only certain memory locations. Also known as sandboxing. The OS will disallow illegal reads and writes, and maybe even log the action attempt.

15. **What is process isolation?**

    When a process is confined and no other process can access resources within its bounds, then it is isolated.

16. **What is the Bell-LaPadula model?**

    Stops information flow from high security to low security in a lattice structure in order to maintain confidentiality only.

    Can't read up
    Can't write down

17. **What is the Biba model?**

    Stops information flow from low security to high security in a lattice structure in order to protect integrity only.

    Can't write up
    Can't read down

18. **What is the Brewer and Nash model?**

    The chinese wall that permits acess controls to change dynamically based on previous activity. Provides integrity by stopping conflicts. You can write to a data set only if you cant read from another one.

19. **What is the Clark-Wilson model?**

    Enforces data integrity by defining each data item. No lattice structure. Instead it has an access control triple where objects can only be accessed through a program/access portal/interface. So it has a separation of duties, good for commercial applications.

20. **What is the difference between a PP and a ST? What's a package?**

    Protection profiles are the security requirements (what the customer wants).

    Security Targets are what the vendors already offer. They can add packages of security features as well.

21. **What is the difference between trust and assurance?** Trust is the level of security built into a system, but assurance is an assessment of the usability of those features in a real world scenario or the degree of confidence in your satisfaction of them.

22. **What is the Goguen-Meseguer model?** A non interference model where subjects and objects of one level don't interfere with subjects and objects of other levels. They are in separate groups.

23. **What is the Graham-Denning model?** Has 8 rules on securely creating/deleting subjects/objects, and provide read/grant/delete/transfer access rights. Defines access rights between subjects and objects.

24. **What is the information flow model?** Focuses on the flow of information, and can also address the type of flow (not just direction). The real goal is to prevent unauthorized information flow.

25. **What is the noninterference model?** How do actions of high security level effect lower security levels? You don't want information leakage from this. This identifies covert channels.

26. **What is the state machine model?** A system that is secure no matter what state it is in. If all possible transitions from one state to another results in another secure state, then it is a secure state machine.

27. **What's the difference between a closed and an open system?** Closed systems are proprietary and will have attack vectors that are less known. It also only works well with a narrow range of other systems (usually from the same company). They can be more secure.

    Open systems are much more easy to integrate and work well with many systems. However, their vulnerabilities are much more well known.

28. **What's the difference between TPM and regular disk encryption?** If you remove the harddrive from the computer that encrypted it with its TPM, it cannot be decrypted at all. You need the TPM chip.

29. **Why is transitive trust a concern?** An subject may gain trust to an object that it shouldn't. You trust the proxy, which trusts websites, so now the subject using the proxy can access blocked websites.

Quizlet

CISSP Chapter 9

Study online at quizlet.com/_2esf7g

1.	**Do applications run in privileged mode or in user mode?**	User mode. When they need higher privileges, they use system calls which are evaluated.
2.	**Give an example of an applet. What are the advantages of applets?**	You go to a website with a mortgage calculator. It sends you an applet that does all the calculations for you. This frees up the web server, gives you a quicker response, and the data remains on your computer.
3.	**How can we detect covert channels?**	Auditing and analyzing log files.
4.	**How can you mitigate EM wire tapping?**	Use shielded cables, conduit, and some physical controls to keep people further from the wires. You can also use TEMPEST technologies like white noise.
5.	**How does a covert storage channel work?**	Write information to a common storage area where another process can pick it up. Sneaky!
6.	**How does ring level effect the queue and resources?**	Processes associated with lower ring numbers take priority. They can also access more resources. If you have a high ring number, sometimes you need to ask a handler or a driver in a lower numbered ring for resources.
7.	**How does the covert timing channel work?**	Manipulating a resource's or process's timing so as to convey information. It also entails studying how long it takes to do things based on different states to deduce information.
8.	**Please explain:** **ROM** **PROM** **EPROM** **EEPROM**	ROM - Read Only Memory (comes already programmed/burned in) PROM - Programmable ROM (can program later) EPROM - Erasable PROM (remove and shine UV light to erase) EEPROM - Electrically Erasable PROM (don't remove, just erase)
9.	**Should BYOD users abide by corporate policies?**	Yes. The same as if you were given that phone by the company.
10.	**What are multiprogramming and multitasking usually coordinated by? What computers use them?**	Multiprogramming is done through specially written software and usually on large-scale systems like mainframes. While multitasking is done by the OS and used on regular PCs and stuff.
11.	**What are protection rings in terms of a protection mechanism?**	These rings organize code in an OS into concentric rings. The deeper into the circle you go, the higher the privilege level associated with that code. Usually OSs use a four ring model.
12.	**What are some concerns of cloud computing?**	Privacy concerns, regulation compliance, adoption of open standards, and if the data can be secured or not.
13.	**What are some disadvantages of applets?**	A website may have malicious applets that are executing code on your system. It could have a trojan horse.
14.	**What are some security concerns of peer to peer solutions?**	Pirating stuff Eavesdropping Consumes all available bandwidth sometimes
15.	**What are some security issues with grid computing?**	The work packets are are potentially exposed to the world. Also, work packets are sometimes not returned on time or at all. It's not viable for time sensitive projects. Finally, an attack on the central grid servers can make the grid computers perform malicious actions.
16.	**What are some vulnerabilites to remote wiping mobile devices?**	Theives can prevent connections that would trigger the wipe function while they dump the data from the phone. Also, it's just a delete operation. That info is probably still recoverable.

17. **What are the five different states a process can be running in?**

Ready
Waiting for its turn to execute.

Waiting
Waiting for a resource. Also called blocked.

Running
Running until complete, until its time slice expires, or its blocked.

Supervisory
When the process must perform an access that has required privileges that are greater than the problem state's.

Stopped
When it's finished or must be terminated. The OS can now reclaim the memory and resources from the process.

18. **What are the four different ways to do register addressing?**

Immediate Addressing

Direct Addressing

Indirect Addressing

Base+Offset Addressing

19. **What are the government's four security modes for systems? What must be in place for all of them?**

Dedicated Mode
System High Mode
Compartmented Mode
Multilevel Mode

They all need a MAC environment as well as total physical control over who can access the computer and even enter the same room as it.

20. **What are the issues with key management on mobile devices?**

Most cryptofailues are due to bad keys, not bad algorithms. Phones rely on poorly-producing RNGs or access better ones through a wireless link. The best storage for keys is on a TPM or HSM, and phones have neither of these usually.

21. **What are the two process states or operating states called?**

Supervisor State
Problem State where privileges are low and requests must be checked.

22. **What are two benefits of process isolation?**

Prevents unauthorized data access since nobody else can read from your confined area.

Protects integrity of the process since nobody else can write to your confined area, and you're not allowed to write to other areas either.

23. **What does the Four Ring model look like?**

Ring 0 - OS Kernel/Memory
Ring 1 - Other OS components
Ring 2 - Drivers
Ring 3 - User code, programs, applications

The top three are privileged
The bottom is user mode

24. **What is abstraction?**

You don't need to know the underlying mechanism of how things work. Just the syntax to get it to work.

25. **What is a client-side attack?**

An attack on a client's computer instead of a network device or a server.

26. **What is a covert channel? What is it vulnerable? What are the two types of covert channels?**

A method used to pass information over a path that is not normally used for information. Since it's not a normal communication path, it probably isn't protected by the system's security controls.

The two types of covert channels are Covert Timing Channel and the Covert Storage Channel

27. **What is aggregation in SQL? What is an aggregation attack?**

Combining information from different tables together into one table.

An aggregation attack combines various low level information to extrapolate higher level information from it.

28. **What is a maintenance hook?**

Entry points into a system that are known only by the developer. Also called a back door. They provide guaranteed access to the system for maintenance if regular access isn't feasible.

29. **What is an example of sequential storage? What's their advantage?**

Magnetic tape drives. They're slow, but extremely cheap for the amount of memory they hold.

30. **What is an inference attack in SQL? How can you protect against it?**

Say you know the total salary given out for a company, and the dates employees started to work. You can infer a specific employee's salary this way.

You can protect against it by blurring the data in the tables. Round salaires to the nearest 100k.

31. **What is a salami attack? How can we prevent them.**

Taking a tiny slice of the money when money is sent, hoping to go unnoticed.

Prevent these by enforcing separation of duties and proper control over code.

32. **What is a state attack?**

Attacks timing, data flow control, and transitions between one state or another.

33. **What is a system call?**

When a process with a higher ring number needs to access resources that a lower ring number has. In other words, when you need more privileged access to complete a task. This is called mediated access.

34. **What is a TOCTTOU attack? What kind of attack is it?**

Time of check to time of use.

When a process checks on an object to see if it's available, it may come back after a few cycles to finally actually use it. You can swap that resource during this time.

It's a race condition attack since you're racing the process to get to the object to switch it before the process uses it. Also known as a state attack.

35. **What is Base+Offset Addressing?**

Give the value stored in one of the registers as the base location from which to begin counting.

36. **What is Compartmented Mode?**

You must meet the clearance level of all the data on the computer.

You need formal access approval for only some of the information on the computer.

You need a valid need to know for that information you have access to.

37. **What is data diddling? How can we stop it?**

Making small, random, or incremental changes to data during storage or transactions.

You can stop it by hashing and decrypting your data after storage or transactions. Use checksums when sending data.

38. **What is data hiding in terms of system security?**

Ensures that data existing at one level of security is not visible to processes of another level at all. It can't be accessed by it.

39. **What is Dedicated Mode?**

You must meet the clearance level for all the data on the computer.

You need formal access approval for all the information on the computer.

You can only get on the computer if all of the data on it falls within your need to know.

40. **What is Direct Addressing?**

Give the address to the value.

41. **What is DMA (Direct Memory Access)? What's the speed like? What's it used for mostly?**

These devices directly exchange data with real memory without the CPU involved. First you send a DRQ request, that the CPU will validate and reserve those memory places for you and you can go HAM in them. When you're done, send a DACK back to the CPU.

This is faster than requiring the CPU to mediate access every time.

Mostly used to permit disk drives, display cards, and multimedia cards to do large scale data transfers.

42. **What is grid computing?**

Think of the PS3. This is when a bunch of nodes work towards a single goal, lending their processing power to complete smaller tasks and send them back. Usually its only when your computer is not in use by you.

43. **What is Immediate Addressing?**

When the value is in the instruction itself.

44. **What is Indirect Addressing?**

Give the address of where the address of the value resides, sometimes on a different page.

45. **What is Interrupt (IRQ)?**

IRQ is an interrupt request. They range in numbers from 0 to 16. You get conflicts when two devices have the same IRQ number.

46. **What is memory-mapped I/O? What should we make sure about it?**

By reading mapped memory locations, you're actually reading the input from the peripheral. If you write to these locations, you are sending output to them.

Make sure only that one device maps into a specific memory address range and that the range is used only for that I/O purpose.

47. **What is Multilevel Mode?**

You need a security clearance for only some of the data on the computer.

You need formal access approval to the information you are cleared for.

You need a valid need to know for the information you can access.

48. **What is multiprocessing?**

Using more than one processor at the same time to execute something.

49. **What is multiprogramming?**

When one process stops to wait on a peripheral, its state is saved and the next process in line begins. This can cause delays on a per process basis, but overall, it's very efficient.

50. **What is multitasking?** Handling two tasks at the same time by switching between them very fast and efficiently.

51. **What is multithreading?** Multiple tasks done within the same process. For example, when you open up three Miicrosoft Word docs, its one process but with three threads.

52. **What is onboarding and offboarding?** When you BYOD to the company and install all the crap they want you to. Offboarding is the reverse and they'll remove their data.

53. **What is phlashing?** Malicious code embedding itself into the BIOS. Also a malicious variation of official BIOS firmware.

54. **What is Phreaking?** Van Eck radiation is reading the electronic emanations from monitors. This can be read from afar and analyzed, which is called Van Eck phreaking. CRT monitors are more prone to this than LCD monitors.

55. **What is real memory?** Also known as main memory or primary memory. IT's the largest RAM storage on your computer.

56. **What is secondary memory?** Storage, as opposed to actual memory. The data is not immediately available. It must be read by the OS and stored in real memory.

57. **What is System High Mode?** You must meet the clearance level of all the data on the computer.

You need formal access approval for all the information on the computer.

Not all the data needs to fall within your need to know, but that's the only data you can access.

58. **What is the difference between an agent and an applet?** Agents are sent from your device to query other ones. Applets are sent from servers to your computer.

59. **What is the difference between Java applets and ActiveX controls?** Java applets can run on any browswer and are sandboxed.

ActiveX uses proprietary Microsoft technology and can run only on Microsoft browsers. It's not sandboxed so it can run different privileged commands.

60. **What is the difference betwen SMP and MPP?** Symmetric Multiprocessing has the processors share the same OS and memory bus.

Massively Parallel Processing houses up to thousands of processors with their own OSs and memory buses.

61. **What is the greatest threat to RAM?** Theft.

62. **What is the part of the OS that always resides in memory so that is can run on demand at any time?** The kernel.

63. **What is the principle of separation of privileges?** Granular access permissions (different permissions for each type of privileged operation).

64. **What is trusted recovery?** Ensures that all controls remain intact in the event of a system crash. In addition, the system lets no opportunities for access when security controls are disabled.

65. **What is UEFI?** Unified Extensible Firmware Interface has replaced the BIOS on modern computers.

66. **What is virtual memory?** A type of secondary memory that the OS manages to make and look like real memory. A page file is an example (writing from memory to disk).

67. **WHat kind of chip is the BIOS usually stored on?** EEPROM so that you can flash it upgrades.

68. **What's the difference between a single state system and a multistate system?** Single state systems only have data of a single classification on it.

Multistate systems will have data of many classifications on it, with protection mechanisms to prevent information from crossing between security levels.

69. **What's the difference between DRAM and SRAM?** DRAM is cheaper but slower. Uses transistors. May retain a slight charge when turned off.

SRAM is faster but expensive. Uses flip-flops.

70. **What's wrong with modems from a security standpoint?** They will allow users to create uncontrolled access points to your network. You should just ban them outright.

71. **Where is meta data stored in terms of data warehouses and datamining?** In a data mart because metadata is of greater value or sensitivity than the bulk of data in the warehouse.

72. **Why are data warehouses and data mining of concern to security professionals?**

Data warehouses have large amounts of information susceptible to aggregation and inference attacks.

Data mining can be used as a security tool to develop baselines for statistical anomaly-based intrusion.

73. **Why is it so hard to protect against DNS attacks? How do we protect against them?**

The attacks take advantage of the normal and proper mechanisms built into various protocols.

Instead of a patch, we need detective and preventative methods like IDS and log reviews.

74. **Why should you attack a caching DNS server instead of an authoritative DNS server?**

It will go unnoticed for a longer period of time. Usually attacks on authoritative DNS servers are picked up right away.

75. **Why should you encrypt SSDs before storing data on them?**

Their wear leveling technology will cause some blocks not to be encrypted. So first encrypt it before anything is saved.

Quizlet

CISSP Chapter 10

Study online at quizlet.com/_2es19g

1. **How can you use white noise to protect your emanations? Where should it be located?**

   Introduce a known pattern or a random pattern that drowns out real communications. Have white noise on the perimeter broadcasting outward so your internal operations work fine.

2. **How do the following motion sensors work?**

   Infrared
   Heat-based
   Wave-pattern
   Capacitance
   Photoelectric
   Passive audio

   Infrared (monitors infrared pattern changes)
   Heat-based (monitors heat patterns)
   Wave-pattern (low or high frequency noise pattern deflection)
   Capacitance (monitors electrical magnetic field around objects)
   Photoelectric (visible light, usually in dark rooms)
   Passive audio (waits for abnormal sounds)

3. **How do you suppress the heat in a fire? The fuel supply? The oxygen supply? Disrupt the chemical reaction?**

   Water
   Soda acid and dry powders
   CO2 and halon
   Halon

4. **How should work areas be classified?**

   The same as your data classifications. If a guy can't go into a room with top secret data, then he probably can't look at top secret documents.

5. **What are badges used for?**

   Identification or for authentication.

6. **What are the four classes of fires and how do you extinguish them?**

   Class A - Normal combustibles (water, soda acid)
   Class B - Flammable liquids (CO2, halon, soda acid)
   Class C - Electrical (unplug, CO2, halon)
   Class D - Combustible metals (dry powder)

7. **What are the four stages of a fire?**

   Incipient, smoke, flame, heat.

8. **What are the four types of fire detection systems?**

   Fixed temperature (sprinkler head melts)
   Rate of rise (how fast temp rises)
   Smoke actuated (CO alarm)
   Flame actuated (based on infrared energy)

9. **What are the four types of water suppression systems?**

   Wet pipe/closed head
   Pipes are already full.

   Dry pipe
   Pipe has compressed air, when fire is detected water shoots out

   Deluge system
   Bigger dry pipe with tons of water, not suitable for environments with electronics

   Preaction system
   Starts off dry, then fills up when smoke is detected. High heat will then activate it. Enables manual intervention to stop the release.

10. **What are the ground rules for securing wiring closets?**

    Never use it as a general storage area

    Keep the area clean

    Don't store flammable items there

    Set up CCTV in there

    Use a sensor to log entries to the room

    Perform regular inspections

    Only administrator has keys to it

    Use sensors to protect the room from heat, water, etc

11. **What are the three groups of physical controls?**

    Administrative (site plans, awareness training, emergency response procedures)

    Technical (CCTVs, fire suppression, alarms, HVAC)

    Physical (fences, locks, gaurds, dogs, man traps)

12. **What are the two types of EMI?**

    Common mode (between hot and ground wires) and traverse mode (between hot and neutral wires).

13. **What are the two ways a physical intrusion detection system can fail?**

    It can lose power and it can fail to communicate to you (a heartbeat sensor checks to see that it can always notify you).

14. **What is a control zone in terms of TEMPEST?**

    The area protected by your faraday cage or white noise. Inside a control zone, your stuff works.

15. **What is a critical path analysis?**

A systematic effort to find the relationships between mission-critical applications, processes, operations, etc.

Example: An e-commerce server sells products over the web. It relies on internet access, computer hardware, electricity, temperature control, storage, etc.

16. **What is a fault and a blackout?**

A fault is a temporary loss in power, a blackout is a prolonged loss of power.

17. **What is an EAC lock?**

Electronic access lock. Uses electromagnet to keep door locked, a credential reader to allow access, and a sensor to know when the door is closed again to lock it.

18. **What is an inrush?**

When you turn on the power and the power coming in is too high at first.

19. **What is a notification alarm?**

Usually a silent alarm that will report to authorities so that they can catch the intruder.

20. **What is a preset lock?**

A physical lock that needs a key. Like at the buildings. Not a cipher lock. Vulnerable to shimming/picking.

21. **What is a sag and a brownout?**

A sag is a temporary drop in voltage, a brownout is a prolonged drop in voltage.

22. **What is a transient and noise?**

A transient is a temporary noise, noise is a power disturbance or fluctuation.

23. **What is clean power?**

Constant, non fluctuating power.

24. **What is generally more effective, a gas discharge system or a water discharge system?**

Gas

25. **What is technology convergence?**

The tendency for technology, while advancing, to evolve and merge features together and come up with do-all equipment. This can result in systems doing redundant tasks, or it may lead to efficiency. But it introduces SPOFs.

26. **What is TEMPEST all about?**

Protects against emanation attacks with anti EMI techniques, like faraday cages and white noise.

27. **What is the difference between masquerading and piggybacking?**

Masquerading is using somebody else's ID card or login credentials.

Piggybacking is the same as tailgating.

28. **What is the fire triangle?**

Fuel, heat, oxygen. In the middle we have the chemical reaction.

29. **What is the functional order in which you want to apply physical controls?**

Deterr
Deny
Detect
Delay

30. **What should an evidence storage system be like?**

Keep it separate from your production data, offline, track activities on it, hash and encrypt all data sets, and only administrators and legal people have access to it.

31. **What's the difference between a local alarm system and a central station system?**

Local alarm system blasts an alarm that can be heard by security guards. Must be anti-tampered.

Central station system broadcasts an alarm to a station which is then heard offsite only.

32. **What's the difference between a spike and a surge?**

Spike is short and acute rise in voltage, surge is prolonged rise in voltage.

33. **What's the relationship between server rooms and human compatibility?**

The less human compatible, the safer it is. For example, oxygen suppression is safer. Very crowded room where it's hard to move is safer. Very cold is safer.

34. **What water suppression system is best suitable for environments with both electronics and people?**

Preaction system

35. **When should you use a surge protector vs an UPS?**

Surge protectors' fuses will blow when there's a surge, protecting your equipment but stopping its power supply abruptly. If your equipment must stay running, use an UPS instead.

36. **Where are wiring closets usually located in reference to each other?**

Same room, different floors. Vertical line going through the building.

37. **Where should a server room be located?**

In the core of a building, away from gas and water lines.

38. **Why can't you use oxygen suppression on burning metals?**

Burning metals produce their own oxygen.

Quizlet

CISSP Chapter 11

Study online at quizlet.com/_2etxj0

1. **Can firewalls block viruses and bad code?** Not usually.

2. **Do brouters attempt to route or to bridge first?** They try to route first. If it can't then it defaults to bridging.

3. **Do WLANs use CSMA/CA or CSMA/CD?** CSMA/CA since they cannot detect wireless collisions.

4. **Explain how WLANs send data using:**
Spread Spectrum
FHSS
DSSS
OFDM

   Spread Spectrum uses many channels at once, in parallel

   Frequency Hopping SS uses many channels, one at a time in series

   Direct Sequence SS uses all channels at once, in parallel

   Orthogonal Frequency Division Multiplexing uses one channel that modulates so it doesn't cause interference but with great throughput. Efficient.

5. **How are the port numbers split up?**
2^16 total ports (65,536)
0 - 1,023 are well known
1,024 - 49,151 are registered
49,152 - 65, 535 are random, dynamic, ephemeral

6. **How does TCP manage flow control?** Using sliding windows. Larger windows for faster transmissions, but only if connection is stable. Smaller windows for shoddy connections.

7. **How does traffic flow in a ring topology?** In one direction. You need a token to send traffic. If the traffic you receive isn't for you, pass it on.

8. **How does VLAN hopping work?** Double encapsulate a packet with two different VLANS, so as one header is stripped off, the next one remains and the packet is sent to a different VLAN by the next switch to read it.

9. **How is polling related to CSMA/CA?** They are opposites. Polling is when the master asks the slaves if they have anything to send, and then grants permission.

   CSMA/CA the slaves ask whenever they need the line.

10. **In TCP/IP, what is IP like? What does it do?** Connectionless and unreliable. It provides route addressing for data packets.

11. **In wireless networks, what are captive portals?** When you log into McDonald's wifi and have to agree to terms. Or at hotels and airports where you have to put in credit card info.

12. **In wireless networks, what's the difference between OSA and SKA?** Open Shared Authentication means no password needed really and usually everything is plaintext. Shared Key Authentication is WEP, WPA, WP2.

13. **Name TCP flags 3-8.** Unskilled Attackers Pester Real Security Folks

   URG
   ACK
   PSH
   RST
   SYN
   FIN

14. **Name three distance vector protocols and one link state protocol.**
Distance vector:
RIP, IGRP, BGP

   Link state:
   OSPF

15. **Whare are the two admission philosophies for NAC** Network Access Control has the preadmission philosophy which wont let a computer join unless they have good security posture.

   It also has the postadmission philosophy which grants and denies access based on user activity based on a predefined authorization matrix.

16. **What are the 4 layers of the TCP/IP model?**
Application
Trasnport
Network or Internet
Link or Network Access

17. **What are the five IP address class ranges? What do they correspond to?**
0000 Class A 0-126
1000 Class B 128+
1100 Class C 192+
1110 Class D 224+ Multicast
1111 Class E 240-255 Reserved

18. **What are the four different infrastructure modes in wireless networking?**

Stand Alone Mode
Just a self contained WLAN, no wired stuff.

Wired Extension Mode
Connects everyone to the wired network.

Enterprise Extended Mode
Same as above, just a bunch of WAPs instead using the same ESSID.

Bridge Mode
Connecting two wired networks to each other. Used when wired bridges are inconvenient.

19. **What are the general wifi security procedures?**

Change default administrator username and password

Change default SSID and disable broadcasting

Use MAC filtering for small WLANS

Use static IP addresses or (or DHCP reservations for small deployments)

Treat WLANS as remote access; use 802.1X and require a VPN link

20. **What are the most common causes of network failure?**

Cable failures or misconfigurations.

21. **What are the most common problems with coax cables?**

Exceed bend radius, using a cable longer than you should, not properly terminated its ends.

22. **What are the most common problems with twisted pair cabling?**

Using the wrong category, using too long of a cable, and too much EMI for UTP.

23. **What are the steps to ARP?**

First check the local ARP cache.
Then broadcast an ARP request.
Then default to gateway which does its own ARP.

24. **What are the three LAN technologies? What is FDDI?**

Ethernet, Token Ring, FDDI.

Fiber Distributed Data Interface is a high speed token-passing technology that has two rings. It can heal itself if a ring goes down by combining into a huge ring.
CDDI uses copper lines instead.

25. **What are the three name layers?**

MAC address
IP addres
Domain name (DNS)

26. **What are the two broad categories of routing protocols?**

Distance vector protocols, which count the number of hops.

Link state protocols, which maintain a topography map and choose a nearest path based on factors like speed.

27. **What are the two methods of disconnecting a TCP session?**

Send FIN packets (FIN, FIN-ACK, FIN, FIN-ACK)
Or just send RST (reset) packet to end it.

28. **What are three benefits and three drawbacks of multiprotocol layers?**

Flexibility and encryption at different levels.

However, there's covert channels, filters can be bypassed, and logical boundaries can be overstepped.

29. **What are two other words for a DMZ?**

Extranet or perimeter network.

30. **What benefits does network segmentation have?**

Boosted performance and better network security.

31. **What devices separate collision and broadcast domains?**

Layer 2 devices separate collision domains (switching).

Layer 3 devices separate broadcast domains (routing, VLANs)

32. **What do ARP and RARP do?**

ARP takes an IP address and finds its corresponding MAC address.

RARP takes a MAC address and find its corresponding IP address.

33. **What do bridges do?**

What layer is it in?

What happens if the networks are different speeds?

Connect two networks together that use the same protocol.

It's a layer 2 device.

If the networks have differing speeds, then it uses store-n-forward as flow control.

34. **What does DNS do? How bout a reverse DNS lookup?**

DNS resolves friendly names to its IP address. Reverse DNS lookup takes an IP address and tells you the website's name.

35. **What does each layer call its information type?**

Application - data stream

Presentation - data stream

Session - data stream

Transport - segment/datagram (TCP/UDP)

Network - packet

Link - frame

Physical - bits

36. **What does ICMP do? What are three utilities of it?**

Used to determine the health of a link. Ping, pingpath, traceroute.

37. **What does IGMP do?**

Allows support for multitasking. You use this to set up groups, join groups, and discover other groups.

38. **What does the physical layer convert?**

Accepts frame from data link layer and convers into bits. Also takes bits and converts into a frame to give to data link layer.

39. **What do gateways do? What else are they known as?**

They connect two different networks that use different protocols. They are known as protocol translators.

40. **What encryption does CCMP use?**

AES

41. **What is 802.11?**

WPA2

42. **What is a CDN? What about client-based CDN?**

Content Distribution Network
Spreading where content is stored around a geographic area for faster loading and for load balancing. Think of Netflix.

Client-based CDN are just P2P programs like BitTorrent.

43. **What is a converged protocol? What are the benefits? Give an example of one.**

The merging of proprietary protocols with open standard protocols.

This can let TCP/IP host those services without special equipment.

Example: FCoE

44. **What is a dead zone in terms of networks? What are the security risks of dead zones? How can we deal with them?**

A network that uses a network protocol other than IP. Since these are rare, most firewalls can't inspect them tofilter them, so they allow either all of their packets in or none. We can encapsulate them into IP packets but we still can't do content filtering on them.

45. **What is a multihomed firewall? IP forwarding?**

A firewall with more than one interface. They should have IP forwarding disabled.

46. **What is an application level gateway firewall?**
What effect does it have on performance and security?

What generation is it?

What layer does it operate on?

It's a proxy firewall that copies packets onto one packet from another, slowing down performance.

However, as it copies it changes source and destination addresses (NAT).

This is a second generation firewall.

Operates on the 7th layer.

47. **What is a stateful inspection firewall?**

What else is it known as?

What generation is it?

What layer does it operate on?

These know some kind of context, so it will know active sessions and what kind of packets go to it.

It's also known as a dynamic packet filtering firewall.

It's a third generation firewall.

It operates on the 3rd and 4th layers.

48. **What is attentuation?**

When a signal degrades since the wire is too long.

49. **What is:**

Bluejacking
Bluesnarfing
Bluebugging

Sending messages to the phone

Stealing the data from the phone

Taking control of the phone, turning on the mic and stuff

50. **What is DNP?**

Distributed Network Protocol

Used in ICS systems. Its an open, multilayer standard.

51. **What is EAP? What about PEAP?**

Extensible Authentication Protocol

An open framework that aims to allow newer authentication technologies to work with older devices to authenticate to each other. Usually plaintext.

Protected EAP encapsulates the EAP methods in TLS.

52. **What is endpoint security?**

The concept that individual nodes should have their own security no matter how secure the network they are in is.

53. **What is FCoE? What layer does it work on? Does it have to be over fiber?**

Encapsulates fiber channel commands over Ethernet on the network layer. Used for NAS and SAN (network storage solutions).

CCoE is the same but with slower copper lines.

54. **What is iSCSI?**

Used for network storage.

55. **What is LEAP?**

Lightweight EAP developed by Cisco. Meant to solve the problems of TKIP for WPA.

56. **What is MPLS?**

Multiprotocol Label Switching
High throughput and performance that handels a bunch of different protocols. Can be used with many networking technologies like SONET and DSL.

57. **What is plenum cable?**

Does not give off toxic fumes if burned.

58. **What is SDN?**

Software defined networking. Separates the infrastructure from the control plane. It's all programmable from a central location. Removes traditional networking concepts like IP addressing and routing.

59. **What is static packet filtering firewall?**

What layer does it operate on?

Why is it weak?

What generation is it?

What else are they called?

Just exams packet headers and filters on rules based on source, destination, and port.

It is weak because it can easily be fooled by spoofed packets.

It operates on the network layer.

It's a first generation firewall.

They are also known as screening routers or common routers.

60. **What is the difference between CSMA and CSMA/CA?**

CSMA just waits for a free line, and then transmits and waits for an ACK.

CMSA/CA will ask for permission to send first, and then sends.

61. **What is the difference between CSMA and CSMA/CD?**

CSMA just waits for a free line, and then transmits and waits for an ACK.

CSMA/CD will send and listen for a collision, and then send a jam signal and re-send after a random period of time.

62. **What is the difference between network monitoring and packet sniffing?**

Network monitoring looks at traffic patters to obtain information about the network.

Sniffing looks at the headers and contents of specific packets.

63. **What is the ping of death?**

Sending a malformed ping of over 65,535 bytes that crashes a system.

64. **What is the security issue with cordless phones?**

It's signal is rarely encrypted so you can intercept it.

65. **What is the session layer responsible for?**

Dialogue control, whether to use simplex or duplex. Establishes and terminates sessions.

66. **What is the transport layer responsible for?**

Managing the integrity of a connection and establishes communications between nodes (think TCP). Also ensures delivery of packets. Sets up the connection for a session.

67. **What is TKIP? How does it work?**

Temporal Key Integrity Protocol was designed to replace WEP without having to upgrade hardware.

This mixes the root key with the IV and uses a sequence counter to prevent replay attacks.

68. **What layer are V.24 and V.35 in?**

Physical

69. **What layer is ARP in?**

Data Link

70. **What layer is ASCII in?**

Presentation

71. **What layer is BGP in?**

Network

72. **What layer is EBCDICM in?**

Presentation

73. **What layer is EIA/TIA-232 in?**

Physical

74. **What layer is FTP in?**

Application

75. **What layer is HSSI in?**

Physical

76. **What layer is HTTP in?**

Application

77. **What layer is ICMP in?**

Network

78. **What layer is IGMP in?**

Network

79. **What layer is IMAP in?**

Application

80. **What layer is in?**

Presentation

81.	**What layer is IPX in?**	Network
82.	**What layer is ISDN in?**	Data Link
83.	**What layer is JPEG in?**	Presentation
84.	**What layer is MIDI in?**	Presentation
85.	**What layer is MPEG in?**	Presentation
86.	**What layer is NAT in?**	Network
87.	**What layer is NFS in?**	Session
88.	**What layer is OSPF in?**	Network
89.	**What layer is POP3 in?**	Application
90.	**What layer is PPP in?**	Data Link
91.	**What layer is PPTP in?**	Data Link
92.	**What layer is RARP in?**	Data Link
93.	**What layer is RPC in?**	Session
94.	**What layer is SKIP in?**	Network
95.	**What layer is SMTP in?**	Application
96.	**What layer is SNMP in?**	Application
97.	**What layer is SONET in?**	Physical
98.	**What layer is SPX in?**	Transport
99.	**What layer is SQL in?**	Session
100.	**What layer is SSH in?**	Application
101.	**What layer is SSL in?**	Transport
102.	**What layer is TCP in?**	Transport
103.	**What layer is Telnet in?**	Application
104.	**What layer is TIFF in?**	Presentation
105.	**What layer is TLS in?**	Transport
106.	**What layer is UDP in?**	Transport
107.	**What layer is X.21 in?**	Physical
108.	**What older model is TCP/IP based on?**	DARPA
109.	**What's the difference between infrastructure mode and ad hoc mode?**	Infrastructure mode requires a WAP. Ad hoc has the devices connect to each other directly.
110.	**Which layers of the OSI model encapsulate a footer and not just a header?**	The bottom two, link and physical layers.
111.	**Which port does BootP use?**	UDP 67 and 68
112.	**Which port does DHCP use?**	UDP 67 and 68
113.	**Which port does FTP use?**	TCP 20 and 21
114.	**Which port does HTTP use?**	TCP 80
115.	**Which port does IMAP use?**	TP 143
116.	**Which port does LPD use?**	TCP 515
117.	**Which port does NFS use?**	TCP 2,049
118.	**Which port does POP3 use?**	TCP 110
119.	**Which port does SMTP use?**	TCP 25
120.	**Which port does SNMP use?**	UDP 161 UDP 162 for trap messages
121.	**Which port does SSL use?**	TCP 443 for HTTP
122.	**Which port does Telnet use?**	TCP 23
123.	**Which port does TFTP use?**	UDP 69
124.	**Which port does X Window use?**	TCP 6,000 - 6,063
125.	**Why don't carries encrypt the data you send out from your phone to the tower?**	CALEA requires communications to be tappable by law enforcement.
126.	**Why do twisted pairs twist wires? What do tighter twists do?**	It protects from EMI and also stops crosstalk. Tighter twists means less crosstalk, so higher speeds can be used.
127.	**Why is WEP weak?**	It uses the same key for all hosts, and its IV is weak.
128.	**Why is WPA weak?**	Although it uses different keys for each host, the same passphrase is used to authenticate to the WAP. You need a 14 character password or better.

1. **Can the ESP in IPsec provide authentication?**

Yes, but limited. The AH does this job better.

2. **Does PPTP support RADIUS and TACACS+?**

No

3. **Does TLS only encrypt TCP? Give an example.**

No, it can encrypt UDP packets as well, as it does for SIP in VoIP.

4. **Do VPNs provide:
Confidentiality?
Integrity?
Availability?**

Yes
Yes
No

5. **Explain NAT vs PAT.**

NAT maps one IP to one IP.

PAT maps one IP to many IPs using IP + Port Number.

6. **Explain the following remote access terms:**
Service Specific
Remote Control
Screen Scraper
Remote Node Operation

Service Specific just gives you access to only a particular service, like email.

Remote Control allows you to control a computer from far away, as though your keyboard and mouse were physically connected to it.

Screen Scraping just sends you a real time image of the remote computer's screen. It's a virtual desktop.

Remote Node Operation is just dial up to a NAC that gives you access to network resources. You're not controlling any other computer.

7. **How can you tell if your IP address is NATed?**

Check the configuration on your router.
Run ipconfig and see if you have a private IP address.
Look up your IP address on whatsmyip and see if there's a discrepancy between that and ipconfig.

8. **How does NAT break IPsec? How do we get around this?**

NAT modifies packet headers which IPsec relies on to prevent security violations.

NAT-Traversal will support IPsec VPNs through EDP encapsulation of IKE.

9. **How does PPTP work?**

The same as PPP, it just tunnels it. So yes it has PAP and CHAP and EAP and all that.

10. **How does VoIP work?**

Encapsulates audio data into IP packets.

11. **In phreaking, what are black boxes?**

They manipulate line voltages to steal long distance services.

12. **In phreaking, what are blue boxes?**

Send 2,600Hz tones over the phone to make free calls.

13. **In phreaking, what are red boxes?**

Simulates the sound of coins being dropped into a pay phone. Usually just tape recorders.

14. **In phreaking, what are white boxes?**

Portable keypad used to control the phone system.

15. **In terms of mail servers, what is Open Relay?**

This is a mail server that does not authenticate senders when sending and receiving mail, so it's opened up to everyone including spammers. They will send a bunch of mail this way.

16. **In terms of security, service, or access mechanism, what is transparency? Why is this a good thing?**

Unseen by users. The less it is seen by users, the better because it's less likely a user will be able to circumvent it or even be aware that it exists.

17. **Is VoIP susceptible to VLAN hopping?**

Yes, you can double encapsulate the packets and get the packets to hop over to a different logical network.

18. **Name four popular VPN protocols. For each of them, tell me:**

What layer does it operate on?
Does it support native encryption?
What networks do they work on?

PPTP operates on layer 2 and does not have native encryption. Can only work with IP networks.

L2F operates on layer 2 and does not have native encryption. Has mutual authentication. Can work on any LAN.

L2TP operates on layer 2 and does not have native encryption, but it can encrypt with L2TP/IPsec. Can work on any LAN.

IPsec operates on layer 3 and has native encryption. Supports transport and tunnel modes. Can only work with IP networks.

19. **S/MIME has signed messages and secure enveloped messages. What do these mean?**

Signed messages provides integrity, authentication, and nonrepudiation.

Secure enveloped messages provide integrity, authentication, and confidentiality.

20. **What are phreakers? What are three things can they do?**

These are people that attack phone systems, or use phone systems to attack you.

They can access your personal voicemail, redirect your messages and calls both ways, make free long distance calls that cost you.

21. **What are the private IP address ranges?**

Class A 10.x.x.x
Class B 172.16.0.0 - 172.31.255.255
Class C 192.168.x.x

22. **What are the two classes of ISDN?**

Basic Rate Interface (BRI)
2 B channels (64Kbps each)
1 D channel (16Kbps)

Primary Rate Interface (BRI)
2 to 23 B channels (64Kbps each)
1 D channel (64Kbps)

23. **What are three benefits of NAT?**

You don't need to lease as many public IP addresses.

Traffic coming into your network can only come in if it was initiated by your network. Intrusion attacks are repelled this way.

Lets your use private IP addresses and hide your network topology from outsiders.

24. **What are three big security risks with IMs?**

Instant Messaging is very susceptable to packet sniffing, can also deliver malicious code, and spoofed to be used for social engineering attacks.

25. **What does APIPA do? What else is it known as? What can an APIPA device connect to?**

Link-local addressing will give you an IP incase DHCP fails. You can only communicate with other APIPA clients within your broadcast domain.

26. **What does PAP do? What about CPAP?**

Authentication protocol for PPP links. Cleartext.

CHAP is the same, except that it encrypts usernames and passwords.

27. **What is a security boundary?**

A boundary between two areas or networks of differing levels of security. Both areas could be secure, or one secure and one not secure.

28. **What is a security issue with PPTP?**

The initial tunnel negotiation process is not encrypted.

29. **What is ATM?**

Asyncrhonous transfer mode cell-switching WAN technology. The use of fixed cell sizes allow ATM to be efficient and fast. It uses PVCs and SVCs.

30. **What is a virtual application?**

An application opened up in a VM. Like running a VM and opening up firefox in it. It doesn't know it's running on a guest OS.

31. **What is a virtual circuit? What are the two types?**

A logical pathway from A to B created over a packet switched network.

A permanent virtual circuit (PVC) is like a dedicated line. It can be closed down when not in use, but started up again as soon as you need it. The path will be the same every time.

A switched virtual circuit (SVC) will be different every time you use one, but the pathway remains the same for the duration of the communication.

32. **What is circuit switching? How does it compare to packet switching?**

This has a dedicated physical pathway from A to B with no variability and no sharing of the line. Usually it carries voice. If the two parties call again, then maybe a different path is created, but this path stays fixed for the entire communication.

It is very connection oriented unlike packet switching. It has constant traffic and it cannot withstand connection loss like packet switching can.

33. **What is Frame Relay? What is at each endpoint? What layer does it operate in?**

A packet switching technology that replaced X.25. It uses permanent virtual circuits (PVCs). It can support multiple PVCs over a single carrier connection. It is connection oriented.

The customer end point has a DTE, the service provider endpoint has the DCE.

Operates on layer 2.

34. **What is mailbombing?**

A DoS attack using spam mail. You're sent so many messages your system crashes or you simply can't accept any real mail.

35. **What is one way TACACS+ authenticates more securely than RADIUS?**

It has two factor authentication.

36. **What is PPP designed to do?**

Support the transmission of IP traffic over dial up or PPP links. It encapsulates the IP packets.

37. **What is SKIP? What layer does it operate on?**

Simple Key Management Protocol

Encrypts sessionless datagram protocols. Designed to work with IPsec.

Functions at layer 3.

38. **What is SMDS?**

Switched Multimegabit Data Service

Connectionless packet swtiching, good for high speed burst traffic and bandwidth on demand.

39. **What is S-RPC?**

Secure Remote Procedure Call

An authentication service that is meant to prevent unauthorized code from being executed on remote systems.

40. **What is swIPe? What layer does it operate on?**

Software IP Encryption

A protocol that uses encapsulation to provide confidentiality, integrity, authentication.

Works on layer 3.

41. **What is the APIPA address range?**

169.254.0.1 - 169.254.255.254 with default Class B subnet mask 255.255.0.0.

42. **What is the general security reason for VLANs?**

Any client on a network that does not need to access other networks for work functions shouldn't be able to at all.

43. **What is tunneling?**

A way to protect the packets of one protocol by encapsulating them in the packets of another protocol.

44. **What is vishing? What about SPIT?**

Vishing is basically phishing but on the phone. They can spoof caller IDs.

SPIT stands for spam over internet telephony. So vishing falls under SPIT.

45. **What is X.25? How did it establish connections?**

AN old and slower packet switching technology that was replaced by Frame Relay. It uses permanent virtual circuits (PVCs) to establish PPP connections.

46. **What kind of connections is RADIUS used for?**

Dial up. Remote.

47. **What kind of links is PEAP used for?**

It's used for securing wireless connections.

48. **What makes IP addresses private?**

All public routers automatically drop packets that have private IP addresses. They cannot be used to communicate over the internet, but only within intranets.

49. **What protocol(s) send mail to mail servers? Which protocol(s) retrieve it?**

SMTP sends it.
POP3 and IMAP retrieve it.

50. **What's the difference between Static NAT and Dyanmic Nat?**

Static NAT permanently assigns a public IP to your device. This means outsiders can initiate communications with your device.

Dynamic NAT allows you to choose from a pool of internal IPs to use with just a few public IPs. It maintains mappings. Outsiders can respond, but not initiate communications.

51. **When using phones, what is callback? What is it's purpose?**

When you call a company and then it disconnects you right away, then tries to call you back immediately. The purpose is so that the toll charges don't fall on the user, but on the company.

52. **Why is tunneling inefficient at times?**

Most protocols already include their own error detection, ACKs, etc. So doing this twice adds more overhead. Also, tunneling creates either larger or more packets which takes up more bandwidth.

Quizlet

CISSP Chapter 13

Study online at quizlet.com/_2et6an

1. **Can a smart card process data?** Yes, it also has a digital certificate on it that you can use to sign emails.

2. **Can LDAP be used to support SSO?** Yes

3. **Describe minimum password age, maximum password age, and password history.** Minimum age is how long you have to keep it for.
Maximum age is when you have to change it.
History means you can't re-use a previous password.

4. **How can you simulate SSO if true SSO technologies and a credential management system are not available?** Use scripted access. Make scripts that will auto log you in everywhere. Passwords for these are usually stored in cleartext, so protect the files they are in.

5. **How do asynchronous tokens work?** You enter your username and password, the authenticating server sends you a challenge number back based on your token ID that will only work on your token. Enter this challenge number into your token and it will spit a one time password back at you. Enter that.

6. **How does device authentication work?** You register a device with your account. A server will check the information of the device, like OS, version numbers, make and model, etc.

   When you log into something from your device, the server will see if you have a device associated with your account, and then check if that's the right device.

7. **How does kerberos protect your credentials?** It uses AES to encrypt them, and timed tickets to prevent replay attacks.

8. **How does SSO increase security? What is it's biggest disadvantage?** Single sign on increases security since user's don't have to write down many passwords over and over. Just one password to access everything. It's convenient too.

   The biggest problem is that now if your one password is stolen, that guy has access to everything.

9. **How does the Kerberos log on process work?** Enter your username and password, it's sent to KDC encrypted with AES.

   Then KDC checks that you're a valid user, and sends you back a symmetric key encrypted with your password hash. Also sends you a TGT that is encrypted and expires.

   When you get the encrypted symmetric key, the client computer will decrypt it with your password hash. You can install the TGT you got until it expires.

10. **How do synchronous and asynchronous tokens differ?** Synchronous tokens are synced with a server, and change passwords every 60 seconds. Both devices must have accurate clocks.

    Asynchronous tokens generate a new password only when it's actually used, based on an algorithm and incrementing counter. This is a one-time dynamic password.

11. **In Kerberos, how are usernames and passwords sent over the network?** Usernames are never cleartext. They are sent encrypted with AES.

    Passwords are actually never sent at all! They are still verified though.

12. **Name six SSO services.** Kerberos, scripted access, OAuth, OpenID, SESAME, KryptoKnight.

13. **Name two non-physical deterrent access controls.** Security policies and security awareness training.

14. **Regarding biometric authentication, what is CER and EER? Is higher or lower better?** Setting the sensitivity of the biometric scanners to the point where FAR and FRR are equal. This gives the Crossover Error Rate, also known as the Equal Error Rate.

    A lower CER/EER is better.

15. **Regarding biometric authentication, what is enrollment and throughput rate? How long is acceptable for each?** Enrollment is the amount of time it takes to register your fingerprint or whatever. 2 minutes max.
Throughput rate is the amount of time it takes to get authenticated. 6 seconds max.

    The more complicated the pattern, the longer it takes for both.

16. **Using Kerberos, after you've logged on and have your TGT, how do you get access to an object?**

Send the TGT back to the KDC and tell it the resource you want to access. It will verify your TGT and check your access control matrix to see if you're authorized, and send you a ST.

Send your ST to the server hosting the resource you want. It will verify your ST with the KDC, and then open a session with you.

17. **What are administrative or management access controls?**

Policies and procedures. These controls focus on business processes, such as labeling data, hiring processes, background checks.

18. **What are CACs and PIV cards?**

Common Access Card
Personal Identity Verification Card

Smart cards used by the US government

19. **What are the different factors of authentication?**

Type 1
Something you know (password or PIN)

Type 2
Something you have (smart card)

Type 3
Something you are or do (fingerprint, keystrokes)
Physiological or behavioral

20. **What are the four components of Kerberos?**

The KDC does the authenticating and stores everyones symmetric keys. The authentication server does the work for the KDC: it has an authentication service (AS) and a ticket granting service (TGS) gives ticket granting tickets (TGTs).

TGTs provide proof of authentication. They are encrypted, expire, and contain the user's IP address. Present this to receive service tickets to access other services.

Service tickets allow you to access a resource. It's encrypted and expires.

21. **What are the four overall steps of access control?**

ID the subject and object
Figure out if the operation is authorized
Grant permission
Monitor and record process

22. **What are the two identify management categories? What is the benefit of each?**

Centralized access control, where a single server does all the authenticating and authorizing. This reduces overhead because it's easier to work with for administrators.

Decentralized or distributed access control, where various devices throughout the network do it.

23. **What does keystroke pattern recognition look for? What's wrong with this authentication technique?**

Flight time and dwell time.

It's subject to many variances due to if you're cold, typing from a different angle, with only one hand, having an injured finger, etc.

24. **What does signature dynamics rely on?**

The pressure of the pen, the stroke lengths, the writing pattern, and flight dynamics. Speed is usually not a factor.

25. **What does the identity and access provisioning lifecycle refer to?**

The creation, review, and revocation of user accounts.

26. **What happens if a RADIUS or TACACS+ or any AAA server gets attacked?**

Only the remote users are affected.

27. **What is a cognitive password?**

Basically the security questions. Stuff about you that can identify you, like mother's maiden name, where you went to school, and the name of your first pet.

28. **What is a compensation access control?**

Used temporarily when a primary access control isn't available. For example, being given an access token until you get your smart card.

29. **What is a corrective access control? What about a recovery access control?**

Modifies the environment to returns systems back to normal to correct problems by a security compromise.

Recovery access controls go a step further and attempt to repair broken things.

30. **What is a directive access control?**

Tries to direct people to comply with policies, like exit signs or supervision.

31. **What is a directory service?**

What are security domains and trusts?

A centralized service that has all the information about subjects and objects. You must authenticate to this directory before performing lookups and queries.

Security domains are groups of users that share the same security privileges. Trusts bridge different domains together so you can access things from other domains. There can be one way or two way trusts.

32. **What is a federated identity management system?**

Separate organizations joining to manage identities between them. Think of SSO, but instead of just in your network, it's for many networks together.

33. **What is a large security difference between RADIUS and TACACS+?**

RADIUS uses UDP unlike TACACS+ that uses TCP.
RADIUS encrypts only the user password while TACACS+ encrypts the entire session.
TACACS+ also separates the three AAA processes.

34. **What is a passphrase?**

IP@ss3dtheEX@M

35. **What is a smart card?**

An ID with an integrated circuit chip. This holds certificates and your asymmetric keys.

36. **What is a token? What are the two types?**

A physical piece of hardware you carry with you that generates dynamic passwords.

The two types of tokens are synchronous and asynchronous tokens.

37. **What is a type 1 and type 2 error? What causes them? How are they measured?**

Type 1 - False rejection
Caused by high sensitivity
Measured by FRR, ratio of false to valid

Type 2 - False acceptance
Caused by low sensitivity
Measured by FAR, ratio of false to valid

38. **What is DIAMETER?**

An AAA service that is an upgrade to RADIUS. It supports VoIP, roaming, uses TCP, IPsec, and TLS.

39. **What is IDaaS? Give an example for it.**

Identity and Access as a Service. It's a third party service that provides identity and access management. It effectively provides SSO for the cloud, especially useful when accessing different SaaS.

As an example, you log into your google account once and you can access all google SaaS this way, from youtube to gmail to google drive.

40. **What is Kerberos? What does it authenticate?**

A third party authentication method that provides tickets. It's a SSO solution and protects your credentials too.

It authenticates clients to servers.

41. **What is OAuth? What about OpenID?**

An open standard SSO service that works with HTTP. It allows you to log into many different services with only one account, like logging into Google and with the same account accessing Facebook and Twitter pages.

OpenID is similar. It can work with OAuth or on its own.

42. **What is the most effective biometric identification? What is the problem with them?**

Retina scans. They can even tell apart identical twins. However, people aren't comfortable with them because they can reveal private conditions, like high blood pressure or pregnancy.

43. **What is the second most effective biometric identification method? Why is it so reliable? What causes it to lose reliability? How can it be fooled?**

Iris scan.

It's reliable because your iris pattern remains largely unchanged for your life and don't reveal medical conditions.

However, pupil dilation from lighting may cause errors

It can be fooled with a high quality image of somebody's eye.

44. **What is the SPOF for Kerberos?**

The KDC. If this is compromised, then so is the symmetric key for every system on the network.

45. **What language is SAML based on? What about SPML?**

Both are based on XML, but SPML is also based on DSML which displays LDAP information in an XML format.

46. **What's a benefit of tokens over your own static password?**

You don't have to rely on remembering it, or writing it down. This is safer.

47. **What's the difference between palm scans and hand geometry?**

Palm readers look at the pattern of veins in your hand. Hand geometry captures a silhouette of your hand and looks at lengths and widths, it is sometimes hard to identify people this way.

48. **When are biometric one to many searches instead of one to one matches?**

If you use a fingerprint as an ID, then it's a one to many search since it compares your fingerprint against a database of everyone's fingerprint until it finds you.

If you use your fingerprint as authentication, then it compares your fingerprint to the one fingerprint it has stored for you.

49. **When is a credential management system useful?**

When your network doesn't support SSO. This will do all the work of entering passwords for you.

50. **When is setting an expiration date for accounts useful?**

When you have contractors that you know will leave the organization. Setting an expiration date will reduce administrative overhead.

51. **Why do federated identity management systems use SAML or SPML?** They use SAML or service provisioning markup language because different networks need to agree on a single language to manage all this stuff together.

Quizlet

CISSP Chapter 14

Study online at quizlet.com/_2ew367

1. **Are foreign words safe from dictionary attacks?**

   No, they use foreign dictionaries too.

2. **How are birthday attacks and rainbow table attacks different?**

   They are the same, it's just that rainbow tables have pre-computed hashes for you to compare. It skips the slow step of calculating hashes, making the process much quicker.

3. **How do capabilities tables and ACLs differ?**

   Capabilities list focus on a subject and his permissions.

   ACLs focus on an object and what people can do to them.

4. **How does rule-BAC differ from role-BAC? What is ABAC?**

   Rule-BAC's most distinguishing feature is that it's rules apply to everyine, like in firewalls. Not just groups. But ABAC can make firewall rules using groups, like preventing managers from accessing something.

5. **How do you implement a DAC model?**

   Make an ACL for each object you own.

6. **How do you protect against birthday and rainbow table attacks?**

   Salt your passwords (add random bits to them before hashing them).

7. **If I have a top clearance, can I access data at the bottom?**

   Usually yes, but you don't have to set up the clearance levels this way. You can require separate clearances for both labels if you want.

8. **If you can't encrypt your password, how can you protect from a sniffer? Tell me three ways to do it.**

   Use a one time password. That way, it won't matter if they can see it. You can also use IDSs to detect sniffers and physical controls to stop people from getting near routers to install them.

9. **In MAC, what's the difference between a hierarchical and compartmentalized environment? Hybrid environment?**

   Hierarchical is just regular vertical MAC labels of security. Compartmentalized is no vertical labels, just side to side. You need a label for need to know and that's it.

   Hybrid is the lattice-based access control that includes both.

10. **Permissions, rights, privileges. Which includes the other two? Which usually refers to what?**

    Privileges are rights and permissions together. Rights usually refer to people.

11. **Three ways to threat model are focus on assets, focus on attackers, and focus on software. Explain the differences.**

    Focusing on assets will look at your objects and try to figure out what the threats are, and use ACLs. More about correcting vulnerabilities.

    Focusing on attackers is easier if you have known enemies, like the US govt. You may miss some attackers this way though.

    Focusing on software is the same as assets, really.

12. **What access control systems are easier to manage for an administrator?**

    Non-DACs since the rest of them can be centrally managed, although they are less flexible.

13. **What are aggregation attacks?**

    These are attacks that combine lots of little bits of information to know more sensitive data about you. Think of the reconnaissance phase of a penetration test.

14. **What are drive by downloads?**

    When you go to a shady website and something downloads without you knowing it. It exploits browser weaknesses.

15. **What are the four access control categories?**

    Rule based
    Role Based
    MAC
    DAC

16. **What does a birthday attack look for in order to crack a password?**

    Hash collisions.

17. **What does SD3+C stand for?**

    Secure by Design
    Secure by Default
    Secure in Deployment +
    Communication

18. **What is a constrained interface?**

    Think of fordham: no volume button showing. Rather than having it there and saying hey you can't do this.

19. **What is a one-upped password?**

    Changing password to password1 or passXword.

20. **What is a side channel attack? What are two types of them?**

An attack against smart cards. Smart cards don't have internal power, but they have a processor. When a smart card is used, it's given power by the reader. The card then sends information to the reader. This information is intercepted and analyzed, and you can discover keys this way.

A power analysis attack is one type, which looks at the consumption of power to extract information.

A fault analysis attack tries to provide the card too little power to collect information little by little.

21. **What is a zero day vulnerability?**

Either an unknown vulnerability (and thus no remedy exists), or a known vulnerability that there still hasn't been a patch for.

22. **What is content-dependent control?**

Can only see specific parts of an object, like views in a database.

23. **What is context-dependent control?**

Requires certain activity before getting permission. For example, you are required to put things in your shopping cart before you are allowed to pay for anything. Date and time can be context too, so you can't use the computer after work.

24. **What is identity based access control a subset of?**

A subset of DAC.

25. **What is last log in notification?**

Shows you the last time you successfully logged on. If you don't recognize it, then you know you've been hacked.

26. **What is password masking? What's it useful for?**

Displaying **** instead of your password when you type it again. Helps against shoulder surfers.

27. **What is the implicit deny principle?**

You don't have permission to so something on a computer unless you are explicitly allowed to.

28. **What is the lattice-based model?**

MAC (comes from using compartmentalization to enforce need-to-know).

29. **What is the separation of duties?**

Sensitive tasks are split into different roles where people can only perform one or the other.

30. **What is threat modeling? When is it usually performed?**

Identifying, analyzing, and categorizing threats based on type and potential danger.

Its performed throughout all stages of a lifecycle.

31. **Why do some organizations rebuild a system of a password is compromised?**

They cannot accept the risk that the attacker has installed backdoors or inserted malicious code. You can trust that the system is secure anymore.

Rather than putting in a more secure password (or even 2FA), it's best to sanitize the system and start over.

Quizlet

CISSP Chapter 15

Study online at quizlet.com/_2evcg6

1. **Explain are the differences between: Security Tests Security Assessments Security Audits**

   Security tests verify that controls are working properly.

   Security assessments are comprehensive reviews that involves a risk assessment, identifies current and future threats, vulnerabilities, and makes recommendations for remediation.

   Security audits are evaluations performed with the purpose of demonstrating the effectiveness to a third party. They are supposed to be impartial and unbaised.

2. **Explain the differences between: Network Discovery Scans Network Vulnerability Scans Web Application Vulnerability Scans**

   Network Discovery Scans are just a kind of fingerprinting. It looks for IP addresses, open ports, what services are running, and any firewalls that lie on the path between the scanner and target.

   Network Vulnerability Scans probe for actual vulnerabilities.

   Web Application Vulnerability scans are more suited towards web applications and does things like fuzzing.

3. **What are the port numbers for these:
FTP
SSH
Telnet
SMTP
DNS
HTTP
POP3
NTP
HTTPS
Microsoft SQL Server
Oracle
H.323
PPTP
RDP**

   FTP 20 & 21
   SSH 22
   Telnet 23
   SMTP 25
   DNS 53
   HTTP 80
   POP3 110
   NTP 123
   HTTPS 443
   Microsoft SQL Server 1433
   Oracle 1521
   H.323 1720
   PPTP 1723
   RDP 3389

4. **What are the three main categories of vulnerability scans?**

   Network Discovery Scans
   Network Vulnerability Scans
   Web Application Vulnerability Scans

5. **What are the three major components of a security assessment program?**

   Security Test
   Security Assessment
   Security Audit

6. **What are the three types of interface testing?**

   API
   User Interfaces (command line, GUI)
   Physical Interfaces (cyberphysical systems, ICS)

7. **What are the two main categories of fuzz testing?**

   Mutation Fuzzing (dumb) where you take previous input values and blindly, slightly alter them and reinput.

   Generational Testing (intelligent) generates data inputs from scratch by developing data models.

8. **What does Metasploit do?**

   Automates known exploit attacks using scripting. Saves you a lot of time.

9. **What is account review used for?**

   Ensure that all users retain only the permissions they are supposed to. Also checks that unauthorized modifications did not occur.

10. **What is a Fagan inspection? What are the 6 steps?**

    The Fagan inspection is a formal method of code review.

    Planning
    Overview
    Preparation
    Inspection
    Rework
    Follow Up

11. **What is a test coverage analysis? What's the formula?**

    This estimates the degree of testing conducted against a piece of software. As in, we tested 80% of all use cases of the software.

    Test coverage =
    (use cases tested / total use cases)

12. **What is dynamic testing? Why is this usually done? What kinds of things can it detect?**

    This is how you test a software while actually running it.

    This is usually done because you purchased the software from a third party and do not have the source code for it.

    This can detect XSS and SQL issues.

13. **What is interface testing?**

    Testing the interfaces between the different parts of a complex application to make sure they function together.

14. **What is misuse case testing?**

    There are ways users may purposely use an application for malicious purposes. So in misuse case testing, you lay out all the possibilities for misuse, and try to exploit the application with manual and automatic techniques.

15. **What is static testing? What kind of tools can do this? When is it a good time to do static testing?**

This is how you test a software without running it, which means you are testing the source code or compiled code. It can find things like buffer overflows.

This can be done manually or with automated tools.

It's good to do static testing throughout the entire development of the software.

16. **What is the purpose of back up verification?**

Testing that all back ups function properly, retain integrity, remain confidential.

17. **When nmap scans a system, what does it mean if a port is open, closed, or filtered?**

Open - The port is open and there's an application actively accepting connections.

Closed - The port is accessible, but there's no application actively accepting connections.

Filtered - Unable to determine since a firewall is interfering.

18. **Within dynamic testing, what are synthetic transactions? What is it used for?**

These are scripted transactions with known results. You run these against the tested code and compare the actual results with the baseline. This is used to verify system performance.

19. **Within network discovery scanning, what are:**
TCP SYN Scanning
TCP Connect Scanning
TCP ACK Scanning
Xmas Scanning

TCP SYN Scanning sends a SYN flagged packet to every port. Half open scanning.

TCP Connect Scanning opens a full connection (SYN then ACK).

TCP ACK Scanning sends an ACK flagged packet to every port to see what it can fool.

Xmas Scanning sends FIN PSH URG flagged packets to see what happens.

Quizlet

CISSP Chapter 16

Study online at quizlet.com/_2ewblc

1. **How can virtualization save on HVAC costs?** You don't need 100 physical servers anymore, just 10 physical ones that host 10 virtual servers each. This also saves on hardware costs.

2. **How can you block a remote wipe signal for a stolen phone?** Remove the SIM card right away, and then put it back in when you're in a faraday cage to dump the data.

3. **How does Microsoft enforce baselines?** They use Group Policy. Change the baseline for the Group Policy and all systems part of that group will have the settings applied.

4. **How does the community cloud model work?** Private cloud shared by a few companies together.

5. **How does the hybrid cloud model work?** You can have a public cloud for everyone (website), and a private cloud for just your company's access (back end).

6. **How does the private cloud model work?** This is a cloud for access by only the single organization paying for it. If they want, to maintain the cloud themselves, they can. Or they can rent resources from a cloud provider (SaaS, PaaS, IaaS).

7. **How does the public cloud model work?** Think of gmail. Anyone at all can use it.

8. **How do you implement baselines with images?** First you set up a computer with all the secure settings you want, and test them. This is the baseline system.

   Next you capture an image of the system and store it on an image server.

   Then have the image server spit it out to all computers.

9. **How is separation of privileges different from separation of duties?** This is what allows you to achieve the principle of least privilege, actually. If privileges are more separated, they can be more granular. Thus you can better give someone only the permissions they need.

10. **In ISO, what is an SAR?** Security Assurance Requirement

11. **In terms of privileges, what is entitlement, aggregation, and transitive trust?** Entitlement is the initial set of privileges a user is given when his account is created.

    Aggregation is the amount of additional privileges the user is given over time.

    You want to ensure you only give nontransitive trusts, if anything. You don't want to give a domain the trust of another plus all of its subdomains.

12. **MTBF vs MTTF?** MTBF assumes you are going to repair it and use it again.

    MTTF is used for things that are thrown out after they fail, like HDDs and tape drives.

13. **Say you buy five licenses of Word for your organization. Why would you install one immediately?** This locks down the other four licenses to your company. Otherwise, if one is stolen, they can install it on their network and you can't use the other four licenses for your company.

14. **Should emergency changes to systems be documented? Why?** Always. This way the change review board can see if it will cause issues. Also, it allows the image to be re-built if anything.

15. **What are RFID tags?** Radio Frequency Identification tags. These are more efficient to use than barcodes, because you can read them from miles away even.

16. **What are the benefits of using images?** You can start all computers from a secure point, you can deploy images very quickly, and you can re-image a computer to fix it quickly. This saves on maintenance costs too.

17. **What are the steps to change management?** Users request a change.

    Then it's reviewed.

    Then it's either approved or not, and roll back procedures are made and tested.

    Schedule a time to enact the change so there's minimal downtime.

    Implement the change.

    Document everything you did.

18. **What are the steps to patch management?** Evaluate new patches to see if they apply to you.

    Test them.

    Approve them.

    Deploy them.

    Verify them.

19. **What goes in a MOU? How does it compare to an SLA?** A Memorandum of understanding lists the intentions of the two companies working together towards a goal. It's less formal than an SLA and does not lay out penalties.

20. **What goes in an ISA agreement?**

An Interconnection Security Agreement lays out the rules for data transmission in terms of how to set up, maintain, encrypt, and close the connections.

21. **What goes in an SLA?**

Performance expectations and penalties for not meeting them. May also have SOC reports, which show how they expect to hit their SLA targets in terms of BCP and disasters.

22. **What is a duress system?**

A distress call plus procedures on how to react to one.

23. **What is a security impact analysis?**

A change management procedure that tries to figure out all the security implications of a change before deploying it.

24. **What is configuration management?**

Ensuring systems are deployed in a consistent manner that is known to be secure.

25. **What is privileged operation monitoring?**

Monitoring administrators and anyone who can do privileged operations to make sure they are not doing anything malicious.

26. **What is the CVE list or CVE dictionary?**

Common Vulnerabilities and Exposure.

A public database of vulnerabilities. Constantly updated.

27. **What kind of backup media is most susceptible to loss over time?**

Tape back ups will corrupt quickly. Keep them away from any and all EMI, like flourescent lights, CRT monitors, etc.

28. **What's the difference between two-person control and split knowledge?**

Two-person control requires the approval of two people to do something.

Split knowledge takes this a step further and makes it physically impossible to do it alone. Both people must do it.

29. **When should you mark data?**

Immediately after creating it.

30. **Which provides the most security?**

SaaS
PaaS
IaaS

IaaS since you have the most control over it and can test and change it all you want. On the other hand, with SaaS you rely on the could provider to have strict controls.

31. **Why is it easy to make and restore back ups of virtual machines?**

They are just files you can copy and paste. Snapshots are also helpful.

Quizlet

CISSP Chapter 17

Study online at quizlet.com/_2exjxw

1. **Can DLP systems decrypt data? Why is this relevant?**

No. This is why attackers sometimes encrypt data before exfiltrating it. It will be undetected.

2. **Explain passive IDS vs active IDS vs IPS**

Passive IDS are not placed in line with traffic. It just sends alerts to you.

Active IDS are not placed in line with traffic, so it can't stop an issue until after it's detected. it sends alerts but also changes the environment to block attacks, like disabling ICMP on the router or changing the ACL on the firewall.

IPS sit directly on the line of traffic and inspect packets before letting them through. This slows down network traffic but it's safer.

3. **How can whitelists block malware?**

Whitelists identify applications by hashing them. If the application has been infected, the whitelist will detect it and block it.

It would also not allow malware to be installed.

4. **How can you prevent against zero day attacks?**

Reduce the attack surface of your system by removing unnecessary systems.

Implement IDSs and firewalls, network and host based.

Use pots and padded cells.

5. **How does a pattern matching DLP system work?**

Looks for patterns and detects them, like XXX-XX-XXXX for social security numbers.

6. **How does a ping flood differ from a smurf attack?**

Ping floods send a million ping request TO the target so it has to respond over and over.

Smurf attacks spoof a ping request FROM the target to a bunch of systems.

7. **How does endpoint based DLP work?**

This detects information stored on drives, removable devices, and sent to printers. It will block prints. It will also scan FTP servers.

8. **How does network based DLP work?**

This detects information leaving a network. The DLP is placed on the edge of a network.

9. **How does the principle of least privilege stop malware?**

Installing applications is usually an administrator privilege. As such, users can't install anything, so malicious code can't either since it assumes the user account.

10. **In terms of auditing, what is an exit conference? When is it held and why?**

An exit conference is when the auditors meet with the organization to discuss their findings and suggestions.

This is done after the audit is complete, but before the report is written and given to the organization. The report is given last so that the exit conference does not alter it.

11. **Name three things can HIDS monitor on individual systems.**

Process calls, infected files, check system files against hashes.

12. **What are change logs? What are they useful for?**

They are part of change management. They record changes to a system. They are useful for restoring systems after a rebuild or in disaster recovery.

13. **What are security logs?**

They log when users access a file, modify it, use resources, etc.

14. **What are SIEM tools? How do they work?**

These are tools that do real time analysis for your network and systems. They use agents that spread throughout the network and report back to the centralized SIEM tool. They also report any alert triggers.

15. **What are some peformance disadvantages of HIDS?**

They use up host resources, slowing them down. Also, they are costly since they must all be monitored equally, where as NIDS have centralized administration.

16. **What are some security disadvantages of HIDS?**

Intruders can detect them more easily than NIDS.

Intruders can steal or modify the logs they save.

17. **What are system logs?**

These log system events, like shut downs, start ups, and when services start and stop.

18. **What are the seven steps of incident response?**

Detection
Response
Mitigation
Reporting
Recovery
Mediation
Lessons Learned

19. **What are the two types of DLP systems?**

Network based DLP
Endpoint based DLP

20. **What are the ways to block DoS attacks? Why are these bad measures?**

Limit the number of open sessions. This will stop eating up the CPU, but still stops legitimate users from connecting.

You can also filter SYN packets based on IP to block an IP address, but many SYN packets will have spoofed IPs all over the place.

You can also reduce the amount of time a server will wait for an ACK after sendings its SYN-ACK.

21. **What does CIRT stand for?**

Computer Incident Response Team

22. **What happens in the detection phase of incident response?**

An IDS or anti-malware could detect something. Or regular users notice something weird.

First responders, usually IT staff, head to the incident to determine if it is a normal troubleshooting issue or if it is an actual security incident that should be escalated.

23. **What happens in the lessons learned phase of incident response? Give examples. What is recommended at the end?**

Any means for improvement at any stage are suggested. It looks to see why, for example, detection was slow, or response was slow, why that was the case, how to fix that, etc. Changes to incident response procedures, controls, and policies are recommended in a report.

24. **What happens in the mitigation phase of incident response? Give a few examples.**

You try to contain the incident. You can isolate the affected computer, or block certain traffic coming in.

25. **What happens in the recovery phase of incident response?**

You try to restore systems to normal functionality.

26. **What happens in the remediation phase of incident response?**

You figure out what allowed the incident to occur by doing a root cause analysis, and then come up with mitigating controls.

27. **What happens in the response phase of incident response?**

Response team members assess the damage and collect evidence.

28. **What is a darknet and what is its purpose?**

A darknet is a portion of allocated IP addresses in your network that are not being used at all. There shouldn't be any traffic in here. Its purpose is to put a host in the darknet that will detect reconnaissance from attackers.

29. **What is a fraggle attack?**

Like a smurf attack, except it uses UDP packets over UDP ports 7 (echo) and 19 (chargen).

30. **What is a honeypot vs a padded cell?**

Honeypots are just fake hosts (usually virtual) with no meaningful data meant to lure you in. Padded cells work with an IDS to transfer intruders to them as soon as they are discovered, and they can't do any damage in there at all (it's padded).

31. **What is a land attack?**

Send a SYN to the target with both its source and destination IP. The system keeps replying to itself this way.

32. **What is an access review audit, and how does it differ from a user entitlement audit?**

Access review audits focus on objects and their ACLs. They will also focus on whether or not accounts are being disabled when they need to.

User entitlement audits focus on the privileges of every user and enforce the principle of least privilege.

33. **What is a smurf attack? How can they be amplified? How can the amplification be stopped?**

Broadcast a ping request, and have it all bounce to the victim since you spoofed his IP. Disable ICMP at your routers to stop this.

It can be amplified if you also send a directed broadcast through the router, so systems on other networks also respond to the ping. To stop this, disable directed broadcast forwarding on your routers.

34. **What is clipping in terms of log monitoring? What's its use?**

A form of sampling that is not statistical. It just collects information that passes a threshold, like the 5th time in a row you enter a wrong password.

It quickly finds items of interest for purposes of legal action or whatever.

35. **What is egress monitoring? How can it be done?**

Monitors outbound traffic to prevent data exfiltration. It can be done with DLP techniques, looking for steganography attempts and watermarking.

36. **What is enticement vs entrapment?**

Enticement is doing what you're allowed to do. If it's not secure, that's fine. It's legal.

Entrapment is tricking people into performing illegal activities or encouraging them to do so. That is illegal.

37. **What is rogueware?**

Fake anti-malware.

38. **What is the difference between monitoring and log analysis?**

Monitoring entails just going over logs to look for something.

Log analysis looks for trends and overall behavior.

39.	**What is the frequency of auditing dependent on?**	Risk. The riskier something is, the more often you should audit it.
40.	**What is the ping of death?**	Send a ping of 64KB.
41.	**What is the primary drawback of using behavior-based IDSs over signature-based IDSs?**	They raise a lot of false alerts.
42.	**What is the primary goal of incident response?**	Reduce the impact of an attack.
43.	**What is the teardrop attack?**	Mangles the packets in such a way that the receiver can't put them back together correctly.
44.	**What is violation analysis?**	This is how you define the clipping level in the first place. Figure out a baseline of expected errors, and set that as the clipping level. Anything above that is a violation.
45.	**What is war dialing? What's the newer form of it like?**	Using a modem to search for a system accepting inbound connections. Newer forms include using VoIP to make calls and listen to find fax machines, mailboxes, human voices, etc.
46.	**What port would an IDS be connected to?**	A SPAN port that has port mirroring.
47.	**Who are typically the first responders to incidents?**	IT staff. They have to then determine if it is a normal troubleshooting issue, and a security incident.
48.	**Why do many incidents go unreported?**	They are not recognized as actual incidents due to poor employee training.
49.	**Why is white box testing more cost-efficient than black box testing?**	Less time needed for discovery.
50.	**Why might auditors issue an interim report?**	The audit process can take very long (months). But if they find something that must be addressed immediately, they will issue an interim report because it's too long to wait until the final audit is completed.
51.	**Why should audit reports be protected?**	Attackers can find the vulnerabilities of your security policy if they have your audit report. Audit reports should be assigned a classification label. Also, you can produce different versions of the same report with different level of detail for different people, like security administrators vs senior management.
52.	**Why shouldn't you turn computers off in the event of an incident?**	They have temporary files and RAM that should be inspected for evidence first.1
53.	**Why should you update your IDS baseline if your network is modified?**	The IDS still thinks you have the old network, so it will raise false alerts on this new network. So you have to train it again on your new network first.

Quizlet

CISSP Chapter 18

Study online at quizlet.com/_2ez5d0

1. **How do differential back ups work? How often can you do them?** They duplicate files since the last full back up, regardless of archive bit. They don't touch the archive bit after this.

   You can do them multiple times a week. But to restore, you only need the latest differential back up.

2. **How does electronic journaling work?** Database back ups are moved offsite in bulk transfers, but frequently and they are stored in back up devices.

3. **How does electronic vaulting work?** Database back ups are moved offsite in bulk transfers. They are not stored in production servers, but in an electronic vault.

4. **How does remote mirroring work?** Production servers at your primary site are mirrored in real time to production servers at the hot site (not back up servers).

5. **How do full back ups work?** They duplicate every file on the system, regardless of the archive bit. Then all archive bits are set to 0.

6. **How do incremental back ups work? How often can you do them?** They duplicate files with an archive bit of 1, which are the files that haven't been backed up since the last full/incremental back up. Then they set the archive bits to 0.

   You can do them multiple times a week. Then to restore, you need to bring all of them over.

7. **In DRP, what is a full interruption?** You literally stop your business processes at the main site and bring them over to the alternate site.

8. **In DRP, what is a parallel test?** You go to your alternate site and recover all processes there as if there was a real disaster.

9. **In DRP, what is a read structured walk through?** The members meet up and mentally pretend to go through a disaster scenario, and team members are asked how they are supposed to respond.

10. **In DRP, what is a read through?** Everyone reads through the plan. This can also identify people who have left, and assigning new roles.

11. **In DRP, what is a simulation test?** This is very much like a structured walk through. You role play a scenario, but then the responses are tested on actual non-critical business processes.

12. **In DRP, what is the telephone tree?** Instead of calling everyone possible, you notify the people under you that there's a disaster and have them notify everyone under them. Then have everyone confirm up that they called down.

13. **In DRP, what's the difference between recovery vs restoration? What teams do them?** The Recovery team works on the activation of an alternate site. They bring businesses and processes back in general.

    The salvage team does restoration once the primary site is safe to go back to. Restoration is fixing the primary site so you can bring the business back there. This is bringing the facility and environment back to normal.

14. **In terms of DRP, what is a service bureau? Where can you access it? Why can they maybe not be a good idea?** This is a company that leases computer time. Access can be remote or on site.

    They will oversell their capacity by gambling that not everybody will need them at once, so you should have a local and a distant service bureau.

15. **In terms of DRP, where should alternate sites be located in relation to your primary site?** Far enough so that they are not affected by the same disaster.

16. **In terms of trusted recovery, what is automated recovery?** The system is able to trusted recover from at least just one failure, like an HDD in a RAID.

17. **In terms of trusted recovery, what is automated recovery without undue loss?** The system is able to trusted recover from at least one failure, but also perform steps to restore itself to normal functionality like restoring corrupted files and verifying key system and security components.

18. **In terms of trusted recovery, what is function recovery?** Can automatically recover specific functions.

19. **In terms of trusted recovery, what is manual recovery?** The system does not fail in a secure state and requires an administrator to manually perform actions to bring it back to a secure state.

20. **What are mobile sites most useful for? Are they usually configured as cold, warm, or hot?** Work groups. Your employees doing similar jobs at others in other locations can now work together for the time being.

    Cold and warm.

21. **What are the benefits of load balancing?** Fault tolerance and scalability.

22. **What are the five ways to test a DRP?**

Read Through

Structured Walk Through/Table Top

Simulation

Parallel

Full Interruption

23. **What are the four types of trusted recovery?**

Manual Recovery
Automated Recovery
Automated Recovery without Undue Loss
Function Recovery

24. **What are the six types of alternate sites used in DRP?**

Cold site, warm site, hot site.
Mobile site, service bureau, IaaS.

25. **What are the three common tape rotation strategies?**

GFS (grandfather son)
Tower of Hanoi
Six Cartridge Weekly

26. **What are the three main techniques used to create offsite copies of database content?**

Electronic Vaulting
Remote Journaling
Remote Mirroring

27. **What are the three main types of back ups?**

Full back ups
Incremental back ups
Differential back ups

28. **What are three benefits of hardware-based RAID over software-based RAID?**

Faster performance, and no need for the OS to be bogged down controlling the RAID.

Has more features, like being hot swappable.

Can logically swap in extra disks to kick in automatically when one fails.

29. **What is a cold site? How long does it take to activate it?**

Has an empty building with electricity and HVAC, just an office environment. No communication connections are set. No preinstalled computing facilities. May take weeks to activate.

30. **What is a failover cluster?**

A cluster of servers where only one works at a time. When one fails, another kicks in automatically.

31. **What is a hot site? How long does it take to activate it?**

Nearly a complete copy of your primary site. It has data, sometimes up to date in real time. It may take seconds or minutes to activate, up to a few hours.

32. **What is a mutual assistance agreement (MAA)? What are three reasons this may be a bad idea?**

Two companies that offer to help each other out in case of disaster.

This is difficult to enforce: one company can back out and say nope I won't help you. They can be sued but so what? You lost.

This also isn't a good idea since both of you may be affected by the same disaster.

Then you also have the issue of confidentiality if you're both operating in the same building with the same infrastructure.

33. **What is a software escrow agreement?**

When you are afraid your software solutions provider will go out of business, this agreement will have them leave their source code with a third party. When trigger events happen (out of business, can't provide tech support, etc) you will be given the source code.

34. **What is a warm site? How long does it take to activate it?**

A building with necessary computing hardware in it, but no current data. All the data must be brought in, and communication lines turned on. Takes about 12 hours to activate.

35. **What is crisis management? How do you mitigate crises?**

This is the panic that sets in when a DRP is kicked in. You can have the checklists and everything, but in a panic people will forget to do things properly.

To mitigate this, you need continuous DRP training.

36. **What is fault tolerance? Give an example.**

The ability for a system to suffer a fault but continue operating.

For example, a RAID-1 array can have a drive fail yet continue to work.

37. **What is RAID-0? How many disks failures are tolerated?**

Striping for performance. No disks can fail.

38. **What is RAID-1? How many disks failures are tolerated?**

Mirroring for fault tolerance. One disk can fail.

39. **What is RAID-5? How many disks failures are tolerated?**

Striping with parity. Requires 3 or more disks. Parity is across disks, so any one disk could fail and it can be rebuilt.

40. **What is RAID-10? How many disks failures are tolerated?**

Stripped mirrors. Each pair is a mirror. One disk per mirrored pair can fail for continued operation.

41. **What is system resilience? Give an example.**

It's similar to fault tolerance, except that it takes it a step further by recovering/correcting the failure.

For example, if a server in a failover cluster fails, another one will pick up in its place (fault tolerance). Then the failed server will be repaired for full functionality again (resilience).

42. **What is the goal of a UPS?**

To provide power for a short time (5-30min) for a logical shutdown or a switch to a generator which takes long to start up.

43. **What is the main difference between incremental and differential back ups?**

Incremental back ups are quick to create, but take longer to restore.

Differential back ups take long to create, but shorter to restore.

44. **What is trusted recovery? In what states can a system fail in?**

Assurance that a system will be just as secure after it recovers from a crash or failure.

Systems can be designed to fail in a fail-secure or a fail-open state, depending on if your company values security or availability more for that particular system.

45. **When a single system fails, what mode should it reboot to?**

It should reboot into user mode. This way it will have less privileges.

46. **When do power generators run out?**

Some will last as long as they have fuel.

47. **Who should have access to your DRP?**

This is a sensitive document. It should be protected with a compartmentalized, need to know basis. Not every member on the team needs to know the entire plan -- just their roles.

However, senior management and other people may have access to the whole plan.

Quizlet

CISSP Chapter 19

Study online at quizlet.com/_2f00kx

1. **"Beyond a preponderance of the evidence" is used for**

   Civil investigations.

2. **"Beyond a reasonable doubt" is used for**

   Criminal investigations.

3. **How do script kiddies attack?**

   They download programs to do it. They don't make their own tools.

4. **What are the four general responsibilities of CIRTs?**

   Determine if an event is an incident, and figure out the scope and amount of damage caused.

   Did any confidential information get compromised?

   Recover from the incident

   Supervise implementation of controls to mitigate this in the future.

5. **What are the nine steps of eDiscovery?**

   Information Governance
   Identification
   Collection
   Preservation
   Processing
   Review
   Analysis
   Production
   Presentation

6. **What are the requirements for court admissible evidence?**

   It must be relevant to determining a fact.

   The fact that the evidence seeks to prove must be material (related) to the case.

   It must be competent, meaning it must have been obtained legally.

   If it's documentary evidence, it must also meet the requirements of best evidence and parol evidence.

7. **What are the six categories of computer crimes?**

   Miligary/intelligence
   Business
   Financial
   Terrorist
   Grudge
   Thrill

8. **What are the three ways to confiscate evidence?**

   Voluntary surrender, subpoena, search warrant.

9. **What are two drawbacks of calling in law enforcement for an investigation?**

   It may become public, which is embarrassing for the company.

   They are bounded by the fourth amendment and other legal requirements that won't apply if the company did its own investigation first.

10. **What does discovery refer to in a trial?**

    Both sides sharing their evidence with each other. However, steps are taken to ensure you are only giving what is asked of you and no more.

11. **What is a federal interest computer?**

    One used by financial institutions, or infrastructure like water, gas, and power systems.

12. **What is a subpoena?**

    A court order that compels an individual or organization to disclose evidence.

13. **What is a testimonial evidence?**

    Someone testifying. It can be direct or circumstantial (necessity of inference).

14. **What is best evidence?**

    A rule that applies to documentary evidence. You can only bring documentary evidence that is in its original form, no copies allowed. Some exceptions are allowed, that copy will be your best evidence.

15. **What is documentary evidence? What are the two evidence rules that apply to documentary evidence?**

    Any written items brought in to prove a fact, like an audit log. This requires a witness to testify to the validity of the evidence.

    The two rules are best evidence and parol evidence.

16. **What is media analysis? How about network analysis? Software analysis?**

    Media analysis recovers all data (including deleted data) looking for evidence.

    Network analysis is harder to get data from, but it includes log files and packets captured during an incident. Also traffic flow information recorded during an incident.

    Software analysis examines source code for back doors, logic bombs, and look at application logs for SQL attacks. This could be a hint that the attacker is an insider.

17. **What is parol evidence?**

    A rule that applies to documentary evidence. When an agreement is put into written form, all terms are in writing and no verbal terms may alter it.

18. **What is real evidence? What else is it known as?**

Evidence that may be brought into the court of law, like a murder weapon, or seized computer equipment.

Also known as object evidence and may be conclusive evidence.

19. **What is remote logging?**

Your audit logs are sent to a remote server and they cannot be modified. Many times they are also hashed and signed.

20. **What is the difference between a business attack and a financial attack?**

Business attacks extract confidential information. The information is worth more than the damage the attack did. Now you have a competitive advantage knowing their trade secrets,, or you've extracted private embarrassing information to expose.

Financial attacks look to steal money, credit card information, or use resources like phones for free.

21. **What should you do if your network is being scanned?**

Log it and save the logs. Scans usually precede directed attacks, so you want these logs as evidence. Scanning isn't always illegal depending on where you live, but it's best to be safe.

22. **What's the difference between interviewing and interrogating?**

Interviewing is gathering information to help you out, from anyone. It's open ended.

Interrogating is when you suspect someone has done something and you try to see if it's true. You have a goal in mind.

Quizlet

CISSP Chapter 20

Study online at quizlet.com/_2f08vq

1. **Do you want higher coupling or lower coupling? Why?** You want lower coupling. This is easier to troubleshoot and update, since there's less dependencies across classes and objects.

2. **Give an example of polyinstantiation.** Say you have the USS Sneak Ship that actually went off course. You want lower users to query it and think it's on track. But when supervisors query it, they will see it's true location.

3. **How are views of a database stored? Why?** Rather than being stored as a separate table, it's stored as SQL commands. This allows you to reduce storage needs and also violate the rules of normalization.

4. **How do compiled languages and interpreted languages differ?** Compile languages (C++, Java) compile into an executable to be distributed. This exe does not show the original code.

   Interpreted lanugages (JavaScript) are distributed as source code, and then end users use an interpreter to execute them. You can view the original source code.

5. **How does API authentication work?** Authorized users are proivded with a complex API key that is passed with each API call. The backend system validates this key before processing a request to make sure the system doing the function call is allowed to do it.

6. **How does the spiral model compare to the waterfall model?** It allows you to revisit all stages in the development process. It is known as the meta model.

7. **How should separation of duties be applied to software development and testing?** Testing should be done by people who did not write the code.

8. **How should systems recover from STOP errors?** In a state that asks you for a password, or in a user mode with restricted privileges.

9. **In a relational DB table, what is:**

   A field?
   An attribute?
   A tuple?
   A record?
   Cardinality?
   Degree?
   Domain?

   Field/Attribute is a column.

   Tuple/record is a row.

   Cardinality is the number of rows.

   Degree is the number of columns.

   Domain is all the allowable values for an attribute.

10. **In DBMS, what is cell suppression?** Hiding a certain cell or field from users.

11. **In DBMS, what is concurrency?** Processes on a database can run at the same time. Concurrency will ensure the database integrity and controls the processes.

12. **In DBMS, what is noise and perturberation?** Putting in false data into DBs to thwart confidentiality attacks.

13. **In DBMS, what is ODBC?** Open Database Connectivity allows different applications to interact with different types of databases through an ODBC interface instead of having to be directly programmed for it.

14. **in DBMS, what is semantic integrity?** Checks that all values are in a valid range and make logical sense.

15. **In DBs, what is a candidate key?** These are sets of attributes that uniquely identify all records. They may change over time. You pick a primary key from here, and this won't change.

16. **In DBs, what is a key? What are the three different kinds of keys?** They uniquely identify records.

    Candidate, primary, and foreign keys.

17. **In DBs, what is a primary key?** This is the actual key chosen that will uniquely identify all records.

18. **In input validation, what is a limit check?** Making sure that the number or character provided falls within a range. Like 1-12 for months.

19. **In input validation, what is escaping input?** When the input has quotation marks, it may be an attack. So the program will replace risky character sequences with safe values.

20. **In software testing, what is a reasonableness check?** Ensuring that values returned by software match criteria that are within reasonable bounds.

21. **In software testing, what is white box, gray box, and black box testing?** White box has the source code and inner workings of the software.

    Gray box has source code but do not analyze the inner workings of the program. They also test the product from a user POV.

    Black box only tests the product from a user POV.

22. **In the ACID model, what is atomicity?** Atomicness! All or nothing transactions. If it can't all be completed, it must be rolled back.

23. **In the ACID model, what is consistency?**

All transactions must be started in an environment that satisfies all DB rules (like primary keys and all that). In addition, all rules must be satisfied when the transaction ends.

24. **In the ACID model, what is durability?**

Once transactions are committed to the database, they must be preserved. You need backup mechanisms like transaction logs.

25. **In the ACID model, what is isolation?**

Transactions must operate separately from each other. If you have two transactions working on the same data, one will lock it until finished, so the other transaction must wait until the first is unfinished.

26. **vIn DBs, what is a foreign key?**

Enforces relationships between two tables, or referential integrity. The foreign key of one table is the still existing primary key of another table.

27. **What are database transactions like?**

If any part of an entire transaction fails, none of it is committed to the database.

28. **What are expert systems? What is its purpose? What are the two components of it?**

A type of knowledge based system (AI). It's purpose is to collect all the information experts know in order to make future decisions.

Knowledge base (all the info, if/then statements)

Inference engine (reasoning and fuzzy logic to make decisions)

29. **What are knowledge based systems? What are two examples of them?**

AI systems meant to simulate human knowledge.

Expert Systems
Neural Networks

30. **What are the five phases of CMM? What is the overall trend?**

Initial
Repeatable
Defined
Managed
Optimizing

The trend is from disorganized development cycles to very defined, organized, and self improving development cycles.

31. **What are the five phases of the IDEAL model?**

Initiating
Diagnosing
Establishing
Acting
Learning

32. **What are the four main values of agile software development?**

Individuals and interactions over processes and tools.

Working software over comprehensive documentation.

Customer collaboration over contract negotiation.

Responding to change over following a plan.

33. **What are the four quadrants of the spiral model?**

Determine objectives, alternatives, constraints.

Evaluate alternatives. Identify and resolve risks.

Develop and verify next level product.

Plan next phases.

34. **What are the security drawbacks of compiled languages?**

Compiled languages are less prone to manipulation by a third party since the source code isn't available, however that also means the software can have a back door or malicious code that you can't detect so easily.

35. **What are the security drawbacks of interpreted languages?**

Since you can view the original source code, you will catch any malicious code. However, anybody can modify the interpreted software without others knowing, so you can embed malicious code in the software yourself.

36. **What are the seven stages of the waterfall model?**

System Requirements

Software Requirements

Preliminary Design

Detailed Design

Code and Debug

Testing

Operations and Maintenance

37. **What do APIs do exactly?**

Allows different web services to interact with each other through function calls.

38. **What do dynamic testing tools do?**

Test the software while running it. This is your only option when buying third party software. Discovers things like XSS and SQL vulnerabilities.

39. **What does the Windows BSOD indicate?**

A detected STOP error. STOP errors are fail-secure states.

40. **What do static analysis tools do in software testing?** Test the code without running it. It tests the source code. It can discover things like buffer overflows.

41. **What happens if your API key is stolen?** Somebody else can interact with a website as if they were you.

42. **What is a fifth generation language?** Creating code using visual interfaces.

43. **What is a first generation language?** All machine languages.

44. **What is a fourth generation language?** Attempts to approximate natural languages, like SQL.

45. **What is a Gantt chart?** Just a schedule that shows time periods in bars. Some of them overlap.

46. **What is agile's primary measure of progress?** Working software.

47. **What is a great security advantage of SQL in terms of access control?** Granularity of permissions. You can limit a user's access to a row, column, or a single cell even.

48. **What is an advantage of using expert systems over real human experts?** Although their only as good as their knowledge base and inference making algorithms, expert systems are never swayed by emotion.

49. **What is a second generation language?** All assembly languages.

50. **What is a security advantage of expert systems and neural networks?** A big task administrators must do is make decisions based on log analysis of giant logs and finding anomalies. These systems can quickly analyze them for the administrators.

51. **What is a STOP error?** When processes execute even though the OS tries to stop it.

52. **What is a third generation language?** All compile languages (high level languages like C++ and Java).

53. **What is cohesion?** The degree to which a class has a single, well defined purpose. Higher is better.

54. **What is coupling?** The amount one class knows about others and depends on others.

55. **What is database contamination? How can you mitigate this?** When you mix data from two different security labels.

Use views and present those to users.

56. **What is database normalization? What are the normal forms?** The process of bringing a database into normal forms, which removes redundancy.

1NF
2NF
3NF
Each is cumulative.

57. **What is database partitioning? How is this a security control?** Splitting up a large table into smaller ones. This helps stop aggregation and inference attacks.

58. **What is fuzzy logic?** Meant to simulate human thought patterns, rather than black and white mathematical computer decisions. It allows for a lot of gray areas.

59. **What is PERT?** Program Evaluation Review Technique is used to estimate the size of a software product (lower, likely, higher bounds) and calculate standard deviation for risk assessment.

60. **What is polyinstantiation? What's its purpose?** When two records/tuples in a database appear to have the same primary key, but different data next to it. The records have different classification labels and this helps against some inference attacks too.

61. **What is the ACID model?** This refers to the four required characterstics of database transactions.

Atomicity
Consistency
Isolation
Durability

62. **What is the feedback loop characteristic of the waterfall model?** Allows you to go back just one stage if you discover errors not found in the previous stage.

63. **What is the idea behind the CMM?** The quality of the software depends on the quality of its development process.

64. **What is the relationship between cohesion and coupling?** Higher cohesion (single purpose) means less coupling.

Lower cohesion (vague purpose) means more coupling since the classes and objects will depend on each other.

65. **What is the security issue with APIs?** Some APIs allow you to do things like place orders or access sensitive information. These may be limited to specific users. They must have good authentication methods to allow this to happen.

66. **What is virtual memory?**

Expanding your primary/main memory by taking part of secondary memory. Like taking a park of your SSD and making it directly accessible to the CPU (page files).

67. **What is virtual storage?**

Turning primary/main memory into secondary memory, like a RAM disk.

68. **What security benefit does OOP have?**

It provides abstraction to the user. It's like a black box. They just know the objects' inputs and outputs, but not the inner workings.

69. **What three functions does DevOps incorporate into one?**

Software development, quality assurance, technology operations.

70. **What two components is SQL split into?**

The Data Definition Language (DDL) which allows for the creation and modification of the stucture (schema).

The Data Manipulation Language (DML) which allows you to update and modify entries, to interact with the data.

71. **Which databases are one to many, and which is many to many? What about one to one?**

Hierarchical models are one to many. One parent, many children.

Distributed models are many to many. All interconnected as a single entity.

Relational databases have a one to one mapping.

72. **Why are time and date stamps important in some DBMS?**

This is important in distributed DBs, since it will employ transactions and then send them out to all other DBs but make sure they are done in the correct order on them.

Quizlet

CISSP Chapter 21

Study online at quizlet.com/_2f0xn7

1. **How can you mitigate viruses spreading over email?** Use content filters which will scan emails for malicious code.

2. **How do encrypted viruses work?** They use a short segment of code (virus decryption routine) which contains the key to load and decrypt the main virus code stored elsewhere on the disk. Each infection uses a different key so it looks like a different virus each time since the main code changes.

3. **How does a companion virus work?** Windows reads commands in .com > .exe > .bat order. These viruses take the names of important OS files like game.exe, but with a priority extension and make game.com. This way when you type GAME into a command line, it will run the infected file instead of the real OS file.

4. **How do file infection viruses work?** They are executables (.exe or .com) that are infected. When run, they damage your system.

5. **How do macro infections work?** These are malicious macro scripts that are automated.

6. **How do multipartite viruses work?** They use more than one propagation technique, such as infecting files plus writing to the master boot record.

7. **How do polymorphic viruses work?** They slightly modify themselves everytime they propogate, copy themselves, or execute. Their signature keeps changing so they are hard to detect.

8. **How do service injection viruses work?** They inject themselves into trusted runtime processes like svchost.exe. They are able to bypass detection in here.

9. **How do stealth viruses work?** These hide themselves by tampering with the operating system to the to fool the antivirus into thinking everything is functioning normally.

10. **How do stored procedures work?** Web servers cannot do SQL commands. Instead, the commands are stored on the database server itself, and the web server just passes parameters to the database server. The SQL commands cannot be modified by anyone but administrators.

11. **How do viruses infect the master boot record?** These records are very small and can't contain much code. So viruses will put a little bit of code in the MBR that will tell it to execute the code in an infected MBR and loads the virus into memory before the OS.

12. **How do worms differ from other malicious code?** They can propagate and copy themselves, eating up your bandwidth.

13. **How do XSS attacks work? What sites do they work on?** Only on sites that allow reflected input.

14. **How do you mitigate damage by new viruses that don't have signatures saved on antiviruses yet?** Use integrity checking software like Tripwire to make sure your system files are okay.

    Enforce stricter user privileges on your systems.

15. **What are four common virus propagation techniques?** Master Boot Record Infections

    File Infection

    Macro Infection

    Service Injection

16. **What are some activities heuristic based antiviruses look for?** Attempts to alter system files (checks hashes).

    Attempts to escalate privileges.

    Attempts to cover their electronic tracks by deleting logs.

17. **What are the three ways to protect against SQL injection?** Web servers cannot do SQL commands. Instead, the commands are stored on the database server itself, and the web server just passes parameters to the database server. The SQL commands cannot be modified by anyone but administrators.

18. **What are three general ways to mitigate IP spoofing attacks?** Packets with a source address from the internal network shouldn't have entered from the outside.

    Packets with a source address from outside the network shouldn't be exiting the network from the inside.

    Packets with private IP addresses shouldn't pass through routers in either direction.

19. **What does adware do?** Just display you a million ads.

20. **What does spyware do?** Watches your moves and reports them elsewhere. It will log things like logins and banking information.

21. **What is an IP probe?** Just a ping sweep. You attempt to ping every address in a range. Systems that respond will be logged for later.

22. **What is are two common ways escalation of privilege attacks are performed?**
Cracking administrator passwords.

Using rootkits.

23. **What is John The Ripper?**
A password cracking tool that automates guesses for you.

24. **What is the master boot record?**
The first sector on a boot disk that will tell the computer the partitions of the disk (OS vs storage vs other) and direct it towards the OS.

25. **What is usually done after an IP probe/ping sweep?**
Port scan to figure out the type of the systems that responded to the ping sweep. This helps you locate web servers and file servers.

26. **Why are most viruses prevalent on Windows machines?**
There's too many different versions of Linux and Unix systems, and viruses must specifically be created for one system at a time. So it's not worth it.