CISSP Notes

Pretty much everything hard that I read or every question I got wrong in my practice exams

- annual loss expectancy is AV asset value times exposure factor EF, times the annualized rate of occurance, ARO. Or ALE = SLE (single loss expectancy) * ARO
- trademarks are for slogans words and slogans, copyrights are for books and videos
- AAA: identification -> authentication -> authorization -> auditing -> accounting
- Strategic -> tactical -> operational from detail and long to short term
- US Can stop terrorism - Unclass, sensitive but unclass, class, secret, top secret
- Public, sensitive, confidential/private
- Control Objectives for Information and Related Technology (COBIT) control framework top 5 principles:
    - Meeting Stakeholder Needs
    - Covering Enterprise End-to-End
    - Applying a single, integrated framework
    - Enabling a holistic approach
    - separating governance from management
- V is the OR symbol
- STRIDE threat assessment : Spoofing, Tampering, Repudiation, Info Disclosure, DoS, Elevation of Privilege
- PASTA (Process for Attack Simulation and Threat Analytics) seven steps:
    - Definition of the Objectives (DO) for the Analysis of Risks
    - Definitional of Technical Scope (DTS)
    - Application Decomposition and Analysis (ADA)
    - Threat Analysis (TA)
    - Weakness and Vulnerability Analysis (WVA)
    - Attack Modeling and Simulation (AMS)
    - Risk Analysis & Management (RAM)
- Decomposition process five concepts:
    - Trust boundaries
    - Data flow paths
    - input points
    - privileged operations
    - details about security stance and approach
- dread rating process out of 100
    - damage potential
    - Reproducibility
    - Exploitability
    - affected users
    - Discoverability
- Quant risk analysis elements
    - Assign asset value - AV
    - Calculate Exposure Factor - EF
    - Calculate Single Loss Expectancy - SLE
    - Assess annualized rate of occurrence - ARO
    - Derive the annualized loss expectancy - ALE
    - Perform cost/benefit analysis of countermeasures

- Value of safeguard is ALE before - ALE after - cost of safeguard (ALE1 - ALE2 - ACS)
- Delphi technique is an anonymous feedback and response process used to enable a group to reach an anonymous consensus.
- Treats & vulnerabilities & asset value = total risk, combination. Controls gap is amount of risk reduced by safeguards. Total risk - controls gap = residual risk
- RMF framework 6 steps:
    - Categorize Info System
    - Select security controls
    - Implement security controls
    - Assess security controls
    - Authorize info systems
    - Monitor security controls
- Symmetric cartography
    - Advanced encryption standard (AES) - 128 block, 128-192-256 key size
    - Rinjdael - variable block, 128-192-256 key
    - Blowfish (often ssh) - 64 block - 32-448 key
    - Data Encryption standard - 64 block - 56 key
    - Idea (PGP) -64 block - 128 key
    - Rivest Cipher 2 (RC2) - 64 block, 128 key
    - RC5 - 32, 64, 128 block, 0-2040 key
    - Skipjack - 64 block, 80 key
    - 3DES - 64 block - 112 or 168 key
    - Twofish - 128 block - 1-256 key
- equation for symmetric keys for p people:p(p-1)/2
- Security Models
    - State Machine Model - Always secure no matter the state
    - Information Flow Model - Focuses on the flow of information
    - Noninterference Model - Subject A should not affect subject B
    - Take-Grant model - Dictates how rights can be passed from one subject to another (subject or object)
    - Bell-LaPadula Model - Prevents leaking or transfer of classified to lower clearance levels where no read-up (simple security) and no-write down (* security)
    - Biba Model - Integrity based model where there is no read-down (simple integrity) and no write up (* integrity)
    - Clark-Wilson Model - allows modifications only through a small set of programs
    - Brewer and Nash Model (Chinese Wall) - Changes access controls based on user's previous activity
    - Goguen-Meseguer Model - members of one subject domain cannot interfere with members of another.
    - Sutherland Model - Defines a set of system states, initial states, and state transitions to maintain integrity and prohibit interference.
    - Graham-Denning Model - focuses on secure creation and deletion of both subjects and objects.
- Levels of TCSEC (Trusted Computer System Evaluation Criteria) (Orange Book)
    - A1 - Verified Protection
    - B1 - Labeled Security (Mandatory protection)
    - B2 - Structured Protection (Mandatory protection)
    - B3 - Security Domains (Mandatory protection)

    - C1 - Discretionary Protection
    - C2 - Controlled Access Protection
    - D - Minimal Protection
- ITSEC levels
    - F0 is lowest, F10 is highest, F7 - F10 have no correlation to TCSEC or CC.
- Red Book (Trusted Network Interpretation of the TCSEC)
    - Four ratings: None, C1 (Minimum), C2 (Fair), B2 (Good).
    - Restricted to networks labeled as "centralized networks with a single accreditation authority"
    - Rates confidentiality and integrity, addresses communications integrity, DoS Protection, intrusion protection and prevention
- Green Book (DoD Password Management Guidelines)
- Common Criteria
    - 7 assurance levels, with the lowest 1 to highest 7 - Functionally tested EAL1, structurally tested 2, Methodically tested and checked 3, Methodically designed tested and reviewed 4, Semi-formally designed and tested 5, Semi-formally verified designed and tested 6, Formally verified designed and tested 7.
- PCI DSS - Payment Card Industry Data Security Standard, requirements for security management, policies, procedures, network arch, software design, other critical protection
- ISO - standards for industrial and commercial equipment, software, protocols, and management
- Certification is first evaluation step, or the technical evaluation of each part of a computer system to assess its concordance with security standards
- Accreditation is next, formal acceptance of a certified config from a designated authority.
- Four phases of certification/accreditation:
    - Definition, verification, validation, and post accreditation.
- Memory related security:
    - Confinement - restricts process from reading and writing to certain memory locations
    - Bounds - the limits of memory a process cannot exceed when reading or writing
    - Isolation - mode a process runs in when it is confined through use of memory bounds
- Security perimeter - boundary that separates Trusted computing base (base that enforces security policy) from rest of the system.
- Reference Monitor - confirms if a subject has right to resource prior to granting access
- Security Kernel - implement functionality of reference monitor
- Common Security Capabilities - Trusted Platform Module, Virtualization, Memory Protection
- CPU Notes
    - Multitasking - cpu handling two or more tasks simultaneously
    - Multicore - more than one core that can operate simultaneously in one CPU
    - Multiprocessing - Multithreading is done In one system (one os, memory) with more than one cpu (Symmetric Multiprocessing SMP) or thousands of processors with own OS and memory resources work on a task together (Massively parallel processing MPP)
    - Multiprogramming - simulated execution of two tasks on a single processor (rarely used nowadays)
    - Multithreading - multiple concurrent tasks are performed within a single process (like running multiple instances of word)
    - Multistate - ability for a system to handle multiple security levels at once with protection mechanisms, as opposed to single state
- Rings - Ring 0 is kernel, ring 1 is components, ring 2 is drivers/protocols, ring 3 is user level programs and apps.

- Dedicated, System high, compartmented, multilevel (lowest security). Each one is a step down from needing full clearance, access approval, and need to know for everything, in that order.
- AMP - asymmetric multiprocessing
  - Processors operate independently but work collectively on a task
- SMP - symmetric multiprocessing
  - All share common processor and memory, also work collectively
- MMP - Massive parallel processing
  - Many SMP are linked together
- BYOD types: Company Owned Personally Enabled, choose your own device, corporate owned, and vdi
- Physical security functional order for controls: Deterrence, denial, detection, delay.
- Power problem terms:
  - Fault - momentary loss of power
  - Blackout - complete loss of power
  - Sag - momentary low voltage
  - Brownout - prolonged low voltage
  - Spike - momentary high voltage
  - Surge - prolonged high voltage
  - Inrush - initial surge of power
  - Noise - steady disturbance or fluctuation
  - Transient - short disturbance
  - Clean - consistent power
  - Ground - grounded wire
- Eight TCP header flags, in order: CWR, ECE, URG, ACK, PSH, RST, SYN, FIN
- Coax cable types - thinnet/10base2 (185 meters, 10Mbps) or thicknet/10base5 (500 meters, 10Mbps)
- 10base5 (10x1mbps, baseband (one signal at a time), 5x100 meters
- Unshielded Twisted Pair (UTP) categories: 1 voice, 2 4mbps, 3 10mbps, 4 16mbps, 5 100mbps,. 6 1000mbps, 7 10gbps
- Enterprise extended infrastructure mode exists for large physical environment wireless with one SSID
- General wireless concepts - Spread Spectrum (Multiple frequencies at same time), Frequency Hopping Spread Spectrum (Constantly changes frequency, minimizes interference), Direct Sequence Spread Spectrum (Uses all frequencies in parallel, high rate of throughput), Orthogontal Frequency-Division Multiplexing (No interference with each other and offers grater data throughput)
- Stateful firewall relies on context (the state of the packet), unlike stateless
- Radius is AAA service, network access server is client
- Discretionary access control - every object has an owner and owner can grant/deny access to other subjects
- Attribute based access control - rules that include multiple attributes (more flexible than rule based)
- Mandatory access control - labels applied to both subjects and objects, relies on classification levels, includes lattice based
  - Hierarchical environment - low to high security, high clearance can access stuff from lower clearance
  - Compartmentalized environment - separate isolation
  - Hybrid environment - both hierarchical and compartmentalized, like lattice

- Non discretionary access controls - centrally managed and controlled
- Fagan inspections for code review:
  - Planning -> Overview -> Preparation -> Inspection -> Rework -> Follow-up
- Static is looking at code, uncompiled. Dynamic is analyzing it during runtime
- Fuzzing types:
  - Mutation fuzzing (dumb) - modifies known inputs to generate synthetic inputs
  - Generational fuzzing (intelligent) - develops inputs based on models of expected inputs
- Segregation of duties = separation of duties + least privilege
- Security impact analysis steps
  - Request -> Review -> approve/reject ->Test -> Schedule -> Document
- Patch Management Program
  - Evaluate -> Test -> Approve -> Deploy -> Verify deployment
- Job rotation and separation of duties prevent fraud not collusion
- Incident is an event that has a negative effect on the CIA of an organization's assets
- Incidence response steps:
  - Detection -> Response -> Mitigation -> Reporting -> Recovery -> Remediation -> Lessons Learned
- Fail-open/fail safe grants access after failing. Fail-secure will default to a secure state after failing.
- Incremental only backups files that have changed, and resets archive bit. Differential does the same but does not reset archive bit (Only needs full + 1 differential to restore).
- Software escrow is to get copies of source code if SLAs are not met or on other conditions
- Recovery - Bringing ops and processes back to working condition, Restoration - bringing facility and environment back to working condition
- DR Plans - Read-Through, Structured Walk-through, Simulation, Parallel, Full-interruption
- Takes about 12 hours for warm site to be ready after disaster
- 80% of states are at moderate to very high risk of seismic activity.
- Electronic Discovery Reference Model: Information Governance -> Identification -> Preservation -> Collection -> Processing -> Review -> Analysis -> Production -> Presentation
- Admissible Evidence Requirements: Must be relevant, fact that the evidence seeks to determine must be material (related to case), and competent (obtained legally).
- Types of evidence: Real (physical objects or conclusive like DNA), Documentary (written items, "best evidence rule" states that documents should be original, "Parol evidence rule" no verbal agreements may modify written agreement), Testimonial evidence (testimony of someone in court or written in a disposition).
- Chain of Evidence required info: Description, time and date collected, location collected from, name of person collecting, and relevant circumstances surrounding collection.
- ISC^2 code of ethics preamble: Safety and welfare of society and the common good, duty to our principals and to each other requires that we adhere, and be seent o adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification.
- Code of Ethics Canons:
  - Protect society, the common good, and necessary public trust and confidence and the infrastructure.
  - Act honorably, honestly, justly, responsibility and legally
  - Provide diligent and competent service to principals
  - Advance and protect the profession
- Ten commandments of computer ethics
  - Thou shalt not use a computer to harm people
  - Thou shalt not interfere with other people's computer work

    - Thou shalt not snoop around in other people's computer files
    - Thou shalt not use a computer to steal
    - Thou shalt not use a computer to bear false witness
    - Thou shalt not copy proprietary software which you have not paid for
    - Thou shalt not use other people's computer resources without authorization or proper compensation.
    - Thou shalt not appropriate other people's intellectual output
    - Thou shalt think about the social consequences of the program you are writing or the system you are designing
    - Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans
- When developing sound systems, you should have these development processes:
    - Conceptual definition
    - Functional requirements determination
    - Control specs development
    - Design Review
    - Code Review walk-through
    - System Test Review
    - Maintenance and Change Management
- CMM vs IDEAL Model (I.. I, Dr. Ed Am Lo(w)
    - Initiating vs initiating
    - Diagnosing vs repeatable
    - Establishing vs Defined
    - Acting vs managed
    - Learning vs optimized
- PERT - Program Evaluation Review Technique is a project scheduling tool that calculates the standard deviation for risk assessment.
- Change management process, 3 basic components: Request, Change, and Release control
- Configuration management components: Identification, control, status accounting, and Audit.
- In a relational database,
    - The cardinality is the rows,
    - Degrees are the columns
    - Domain is the allowable values that attribute can take
    - Candidate key is subset of attributes that can be used to uniquely identify any record in a table (Each table can have one or more).
    - Primary key is selected from set of candidate keys and used to uniquely identify the records in a table(Each table can only have one).
    - Foreign Key is used to enforce relationships between two tables (AKA Referntial integrity).
    - Database normalization is to create well-organized and efficient databases, three forms 1NF, 2NF, 3NF. Reduces redundancy, higher levels are more efficient.
- Database transactions have four characteristics (ACID MODEL):
    - Atomicity - "all or nothing affair"
    - Consistency - Begin and complete operating in an environment that is consistent with database rules
    - Isolation - Transactions must operate separately from each other
    - Durability - Database transactions must be durable and preserved.
- Multilevel Security Databases - contains information at different classification levels through the use of labels or views

- Concurrency - edit and view control so that info is always correctly written or read.
- Polyinstantiatiation - when two or more rows in the same relational database seem to have the same primary keys but different data for use at differing classification levels.
- NOSQL - database or models that are not relational
    - Key/Value stores - store info in key/value pairs
    - Graph Databases - use nodes to represent objects and edges to represent relationships
    - Document Stores - store info in key/documents (more complicated than just values)
- Knowledge-based AI system types
    - Expert Systems
        - Embody accumulated knowledge of experts and apply it in a consistent fashion to determine future decisions
        - Expert systems uses if/then statements to form decisions based on previous experience of human expert
    - Machine Learning
        - Use analytic capabilities to develop knowledge from datasets without direct application of human insight
        - Type types: Supervised (correct answers known) and unsupervised learning (Correct answers unknown).
    - Neural Networks
        - Chains of computation units are used to imitate the biological reasoning process of the human mind.
- Dev, QA and IT Ops are three elements of DevOps
- Virus Technologies
    - Multipartite Viruses - use more than one propagation technique to infect victims
    - Stealth Viruses - hides themselves by tampering with OS system
    - Polymorphic Viruses - modify code when travelling from one system to another
    - Encrypted Viruses - use crypto techniques to avoid detection
- Time of check to time of use (TOCTTOU or TOC/TOU) - make sure there is not a big delay between checking access and resource requests
- Rootkits are used for privesc.
- Three ways to limit SQLi: Use prepared statements, perform input validation, and limit account privileges
- XSS is only effective against reflected input

- Hewlett Packard Enterprise

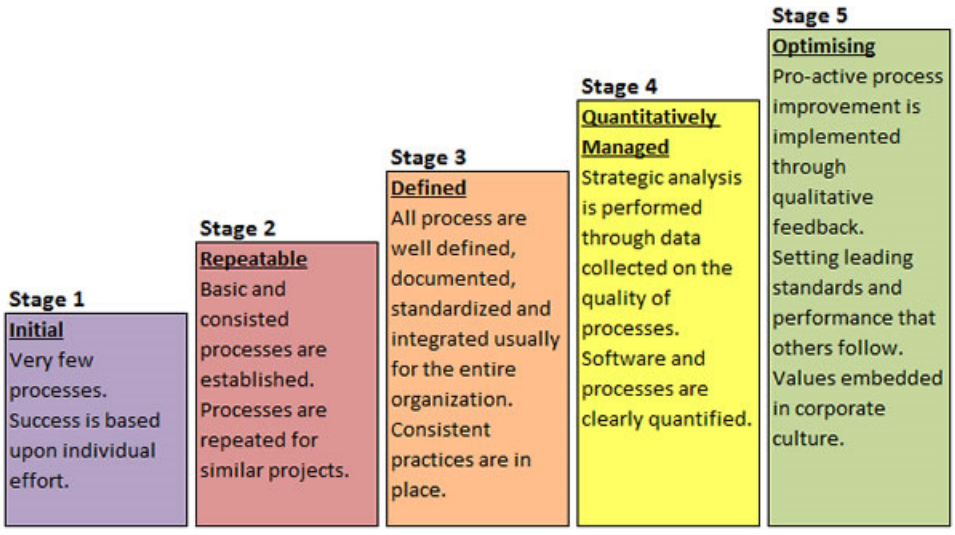
BREAKDOWN OF COMMON RAID LEVELS

RAID LEVEL	METHOD	HARDWARE / SOFTWARE	MINIMUM # OF DISKS	COMMON USAGE	PROS	CONS
JBOD	SPANNING		2	INCREASE CAPACITY	COST-EFFECTIVE STORAGE	NO PERFORMANCE OR SECURITY BENEFITS
0	STRIPING		2	HEAVY READ OPERATIONS	HIGH PERFORMANCE (SPEED)	DATA IS LOST IF ONE DISK FAILS
1	MIRRORING		2	STANDARD APP SERVERS	FAULT TOLERANCE, HIGH READ PERFORMANCE	LAG FOR WRITE OPS, REDUCED STORAGE (BY 1/2)
5	STRIPING & PARITY		3	NORMAL FILE STORAGE & APP SERVERS	SPEED + FAULT TOLERANCE	LAG FOR WRITE OPS, REDUCED STORAGE (BY 1/3)
6	STRIPING & DOUBLE PARITY		4	LARGE FILE STORAGE & APP SERVERS	EXTRA LEVEL OF REDUNDANCY, HIGH READ PERFORMANCE	LOW WRITE PERFORMANCE, REDUCED STORAGE (BY 2/5)
10 (1+0)	STRIPING & MIRRORING		4	HIGHLY UTILIZED DATABASE SERVERS	WRITE PERFORMANCE + STRONG FAULT TOLERANCE	REDUCED STORAGE (1/2), LIMITED SCALABILITY

What Happened to 2-4 and 6-9?

The RAID levels described above are the most common levels used in enterprise scenarios. The levels in between are highly specialized and only make sense in very specific scenarios.

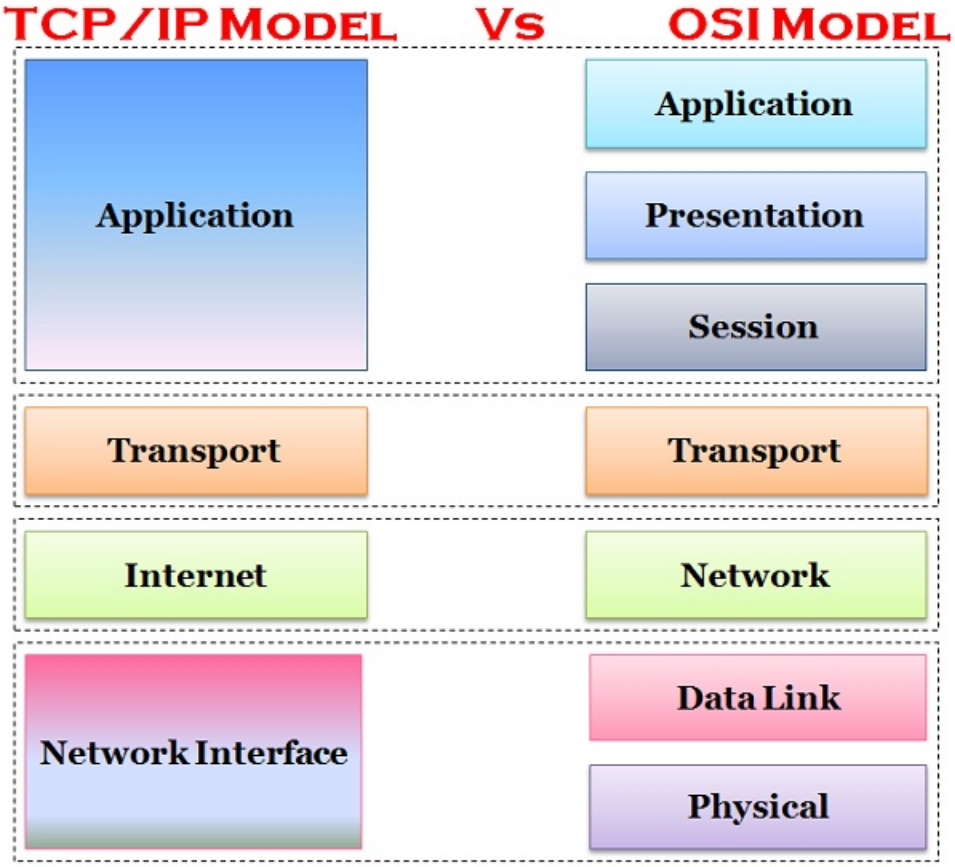
- **Capability Maturity Model Maturity Levels**

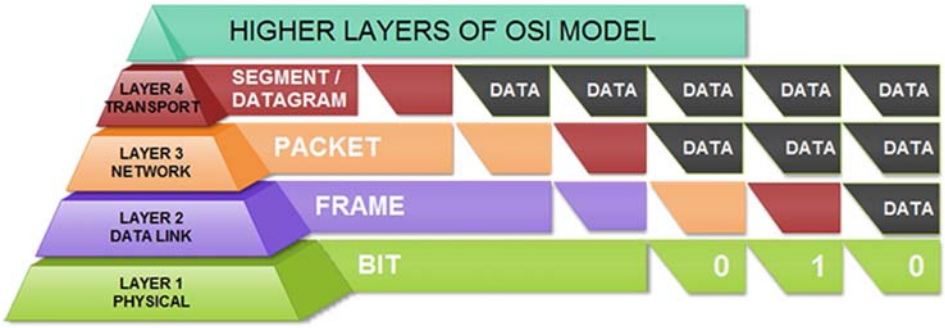


- Fire Extinguisher types:

- **Classes**
  A Common WATER, SODA ACID (take away temp)
  B Liquids----GAS/CO2, SODA ACID (takes away fuel)
  C Electrical-----GAS/CO2 (displace O2)
  D Metals----DRY POWDER

  WATER suppress temperature
  SODA ACID reduces fuel supply
  CO2 reduces oxygen
  HALON chemical reaction
  Fire distinguishers should be 50 feet from equipment and toward the door
  Heat





Stuff I learned from quizzes:

- Domain 1 (Security and Risk Mgmt):
  - CALEA? Yes communications assistance to Law Enforcement Act

    - final step of quant risk analysis is cost/benefit
    - prudent man rule requires senior execs to take responsibility of due care.
    - US Department of commerce implements us-eu shield agreement
    - GLBA is for financial stuff
    - FISMA applies to gov contractors - Federal Information Security Management Act - Requires federal agencies to implement an ifosec program.
    - Economic espionage act fines and jails of those stealing trade secrets
    - ACLs are used for determine user auth levels
    - MTO = Maximum Tolerable Outage
    - RTO = Recovery time objective
    - SOC 2 service organization control audit program includes business continuity controls
    - fourth amendment is to protect against privacy
    - electronic vaulting is part of disaster recovery, not business continuity
    - NIST is responsible for standard and guidelines for federal systems
    - project scope and planning includes 4 actions, structured analysis, creation of BCP, assessment of resources, and analysis of legal and regulatory landscape
    - info disclosure attacks rely on revelation of information
- Domain 2 (Asset Security)
    - clearing is preparing media for reuse
    - COBIT is needed for business owners to apply security controls
    - Classification levels for US Gov - confidential for cause damage, secret is serious, top secret is grave damage
    - value of media often exceeds cost of the media
    - erasing only removes link to file and is most risky, clearing and purging is more secure, degaussing is ok too.
    - How US Govt classifications relates to private companies: TOP secret = confidential Secret = private Confidential = sensitive
    - group policy monitors baselines
    - GDPR needs to protect data against accidental destruction but does not require data at rest encryption
    - encrypting and labelling is better for only sensitive emails.
    - issue is mishandling of drives by third party, not data remanence for when sending drives to be shredded.
    - cost is not directly included in determining classification, but who can access is important
    - California Online Privacy Protection Act (COPPA) is a law that needs privacy policies if they collect info on California residents
- Domain 3 (Security Architecture and Engineering)
    - Brewer Nash is for dynamic changed access controls, review all models like biba, etc.
    - DSA RSA and ECDSA are approved for DSS
    - MD5 has collisions but SHA256 is good.
    - ESP provides confidentiality and integrity for IPSEC
    - Diffie Hellman allows for exchanging of symmetric encryption
    - Protection Profiles (PPs) specify product security requirements for Common Criteria
    - Kerckhoff's principle says crypto system should be secure even if open source
    - Fair Cryptosystem key escrow requires 2 parties
    - ready state is for tasks prepared to execute but cpu not ready. Waiting is for blocked by external
    - EAL1 applies when functionally tested, lowest level of Common Criteria

- Multistate systems are for different security class simultaneously
- caesar cipher is a shift cipher
- verification process validates controls by third party, not accreditation which is more of a formal declaration to operate in a specific environment
- If you must reuse an SSD, use encryption on the disk
- known plaintext attacker has copy of encrypted message with plaintext message. Chosen-plaintext is when the attacker can obtain ciphertexts for chosen plaintexts. Chosen-ciphertext is when you can obtain decryptions of chosen ciphertexts.
- x509 is for digital certs
- multithreading is when multiple tasks are run within a process
- transposition cipher does not change frequency distribution of english language
- heartbeat sensors sends alerts occasionally
- blowfish uses variable key lengths
- RSA is asymmetric and therefore can be used for digital certs
- Halon uses a CFC suppressant and was banned as it depletes ozone
- TLS uses symmetric ephemeral session key
- When only executable code is given to a vendor, that's like a cloud environment, which is PAAS (IAAS gives you OS control too)
- Ideal humidity in a server room should be 40-60% due to static electricity
- serial numbers are used by CRL (Certificate Revocation List)
- covert timing example: rhythm of morse code
- Sometimes if the cost is too great to secure an remote access vulnerability, move it to a secure network.

- Domain 4 (Communication and Network Security)
  - ftp operates on 20 and 21 TCP
  - CHAP is used by PPP servers to authenticate, PAP does too but it is unencrypted.
  - RADIUS was designed to support dialup but supported for VPN. ESP and AH are IPsec and do not provide authentication
  - # of zones protected behind firewall = how many tiers
  - DNS poisoning changes dns to ip mappings, dns spoofing just beats valid results from a DNS server
  - Screen scraping just copies display, does not allow for control
  - Multilayer protocols may have covert channels, may bypass filters and logical boundaries (think serial SCADA link)
  - SPIT is spam over internet telephony and targets VoIP
  - PRI or primary rate interface can use 2-23 64 kb channels with a max bandwidth of 1.544 Mbps
  - FDDI or Fiber Distributed Data Interface is a token-passing networker that uses rings with traffic flowing in opposite directions (Token ring uses tokens but not in a dual loop). SONET deals with fiber and sending multiple optical streams over it
  - PPTP, L2F, L2TP and IPSEC are the most common VPN protocols
  - Private branch exchange (PBX) systems are typically standard telephones and do not carry encryption, so physical security is best solution.
  - Firewalls will stop at the first matched rule
  - A data streams are associated with app, presentation, and session. (Highest to lowest are Data streams, segments, packets, frames, and bits)
  - servers may talk to each other within virtual environment, so you have to actively think about packet logging

- T3 line is capable of ~45 Mbps, T1 is 1.544Mbps , ATM is 155Mbps, ISDN is 64 or 128 Kbps
- Bluetooth pins can only be 4 digits long
- PPP is used for dialup!
- teardrop uses fragmented packets to exploit how a system handles reassembly
- ethernet uses BUS topology as they can collide
- yes cat 3 provides 10MBPS, cat 5 is 100Mbps , 5e is 1000Mbps, cat 6 is 1000Mbps
- WEP is weak due to static common key and limited IV, does not use asymmetric encryption
- DKIM allows domain identities to verify email

- Domain 5 (IAM - MY WORST SECTION)
  - Capability tables list privileges assigned to subjects and the objects they can access.
  - On-prem 3rd party identity service can integrate with IDaaS solution, especially with AD.
  - Kerberos encrypts messages with secret keys.
  - Kerberos auth process: User provides auth, Client/TGS key generated, TGT is then generated, client/server ticket generated, then user accesses service.
  - A landline call is a somewhere you are, mobile is something you have.
  - Kerberos uses realms and proper type of trust for AD needs to connect to a K5 domain is a realm trust. Forest trust is a transitive trust between two forest root domains
  - TACACS+ AAA protocol is most commonly used
  - AD Federation Services, Central Auth Services, and Kerberos are all SSO. Radius is not.
  - yes client in Kerberos logins use AES to encrypt user and pass
  - Yes KDC uses user's pass to generate a hash and uses that to encrypt a sym key. Sends both encrypted sym key and time-stamped TGT to client.
  - Client needs to install TGT for use and needs to decrypt sym key user a hash of user's password before a TGT can be used
  - Retina scans can reveal medical conditions
  - MAC systems are based on a lattice model, biba also is based on a lattice model/MAC
  - Resource based access controls match permissions to resources like storage volumes
  - Radius uses UDP and encrypts passwords by default
  - AS = authentication services in kerberos (TS does not exist)
  - Phishing is not a threat to access control mechanisms, it is a threat to users.
  - LDAP DN can have plus and commas, no semicolons.
  - A stored biometric factor is called a reference profile or template.
  - TLS for SAML provides confidentiality and integrity, with digital signatures authentication is also provided.
  - Hybrid cloud and local auth system ensures outages are handled for availability purposes
  - Service Provisioning Markup Language (SPML) used to allow platforms to generate and respond to **provisioning** requests.
  - Google's federation allows SSO but goes beyond it, including rights and cert management.
  - Yes port 636 is default for LDAPS (over SSL or TLS, normal LDAP is 389), 3268 and 3269 (secure) are for global catalogs
  - X.500 covers directory services, Kerberos is described in RFCs
  - Active Directory Domain Services (ADDS) is based on LDAP, AD also uses kerberos
  - OpenLDAP stores passwords in the clear
  - Type 2 error is when an invalid subject is incorrectly authenticated (like to someone else's account, even if you have an account).
  - RADIUS uses TLS over TCP, not native UDP
  - MAC systems do not allow rights to lower class levels (secret cannot access unclass by default).

- Simple Authentication and Security Layer (SASL) for ldap provides secure authentication
- Phishing attacks could happen if relying party provides redirect to openID provider
- Recovery controls are like RAID
- LDAP DNs should be most specific to least specific (ben, sales, example, com)
- if time is more than 5 mins out of sync Kerberos won't receive any new tickets.
- Kerberos, kryptoknight, and sesame are all SSO systems.

- Domain 6 (Security Assessments and Testing - MY SECOND WORST SECTION)
  - mutation testing modifies programs in small ways to test if they will fail
  - IPS is a mechanism like hardware, software, firmware based control system. Specs are documents like policies or designs.
  - type I audits do not cover period of time, only a single point in time unlike type II
  - WPA2 enterprise uses RADIUS auth, not passwords
  - causing alarms on IPS with wireless scanning is intentional, not a problem
  - generational fuzzing relies on models. But mutational fuzzers are dumb
  - MTD is maximum tolerable downtime, not helpful with testing backups.
  - TCP connect scans can be done without packet creation privileges.
  - synthetic monitoring uses emulated or recorded transactions to monitor behavior.
  - Real user Monitoring is passive monitoring that captures user behavior
  - important part of app threat modeling is threat categorization. Assesses attacker goals and where controls should be placed.
  - passive scanning can help identify rogue devices by capturing MAC addresses
  - bluetooth active scans can determine both the strength of the PIN and what security mode the device is operating
  - regression testing ensures that changes have not introduced new issues.
  - key indicators tell how risky an activity is and are used to monitor high risk areas.
  - how vulnerability data should be stored and sent is critical to address during planning for a pen test
  - code coverage testing requires that every function, statement, branch, and condition be called.
  - API, ui, and physical interfaces are important during software testing. Network interfaces are not.
  - CVE provides consistent reference for security vulnerabilities
  - NIST 800-53A (like SEA of controls) covers methods for assessing and measuring controls
  - TCP connect is 3 way handshake, TCP ACK disguises as active control
  - ITIL is for IT service management.
  - NIST SP 800-137 (like LE(E)T monitoring) outlines the process for organizations that are maintaining an Infosec Continuous Monitoring (ISCM). Define, establish, implement, analyze, report, respond, review, and update.
  - Regression testing prevents recurrence of issues.
  - test coverage report measures how many test cases have been completed from a functional perspective.
  - validation is necessary after vulnerability scanner finds an issue.
  - fagan inspection process: Planning, overview, preparation, inspection, rework, follow up
  - Not having enough log sources isn't a key consideration in log management systems
  - Common Platform Enumeration of SCAP provides a way to refer to OS and system components.
  - Rebooting a windows machine results in an information log entry.

- Authenticated scans use a read-only account to access config files, allowing for more accurate testing
- shared sym key can lead to repudiation issues.
- fuzz testers automatically generate input sequences to test an application.
- statement coverage tests verify that every line of code was executed
- after nmap you do more detailed vuln scans
- x11, ssh open indicate linux instance
- nmap scans 1000 tcp and udp ports, not just "well known ports" by default.
- manual code review is the best option to understand context and business logic.
- misuse case diagrams use language like threatens and mitigates, which is beyond typical use case diagrams.
- specs are documents associated with system being audited
- when addtl tools are installed, pentesters use them to gain addtl access.

- Domain 7 (Security Operations)
  - failover cluster is when two servers are both configured and is ready to fail over.
  - manual recovery approach does not fail to a secure state and requires an admin to manually restore operations
  - pseudoflaw is a false vulnerability in a system that may attract an attacker
  - social media is typically used for botnet
  - Verify security clearance and business before granting access
  - forensic disk controller write blocks, intercept write commands, prevents modification of data, return data requested by read, returning access-significant info from device, and reporting errors back to host.
  - Yes, darknet is a monitored network without any hosts
  - Hacking is considered a man-made disaster
  - Checklist is least disruptive, even more so than a tabletop exercise.
  - Grandfather/father/son, tower of hanoi, and six cartridge weekly are all backup media rotation approaches.
  - public cloud computing model is like AWS EC2 instances where infrastructure is shared.
  - CISRT includes reps from public affairs, engineering, legal, infosec, and senior management
  - entitlement refers to permissions upon first grant
  - ISC^2 code of ethics only applies to members of ISC^2, but you do have to report possible violations.
  - syn flood is when you send lots of syn packets without responding to syn/ack. Smurf is ddos is done via spoofed ICMP broadcast. Fraggle is spoofed UDP to broadcast.
  - interviews are when you are not a suspect but have information.
  - electronic vaulting moves database backups from primary to backup site
  - after DR, goal is to restore normal business ops in primary facility
  - evidence must be relevant, material, and competent (legally obtained)
  - software escrow is best defense against software company going out of business
  - netflow data is best to analyze after bot infection, especially encrypted ones.
  - ping of death was more data than allowed in icmp payload, similar to buffer overflow
  - enabling syn-ack spoofing at firewall is an effective way to block a syn flood, as the listener never sees the syn traffic unless it is legit
  - PAAS - customer supplies code that vendor executes on its own infrastructure.
  - companies need to preserve evidence when they believe a threat of litigation is imminent
  - fourth amendment is against unreasonable search and seizure
  - analysis of app logs is part of software analysis

- public domain software has no limitations of reuse
- (System Center Config Manager) SCCM allows for evaluation of windows workstation configuration status. System Center Operations Manager (SCOM) ... is for monitoring health and performance

- Domain 8 (Software Development Security)
  - coupling is a description of level of interaction between objects. Cohesion is strength of relationship between methods of the same class. When you are developing object oriented mode, you want high cohesion and low coupling.
  - release control process includes acceptance testing
  - BSOD is a fail secure example
  - software threat modeling is designed to reduce number of security related design and severity of other flaws. You cannot reduce number of threats as it is external.
  - primary storage refers to memory. Hard drives are secondary storage.
  - repeatable is in the second stage of SW-CMM
  - defined stage of CMM has standardized processes
  - optimising is highest level of CMM, it goes initial -> repeatable -> defined -> managed ->optimising
  - referential integrity ensures records exist in secondary table via foreign key
  - change control process provides organized framework where developers can create and test solution prior to rolling it out in prod
  - timing and storage are covert channel classifications
  - inference is finding out more sensitive info through aggregation. Aggregation is the actual process of putting together the info.
  - Pass around reviews are typically done via email, allowing developers to review code at different times. Fagan review is much more formal and needs both the dev and team at the same time.
  - multipartite viruses help propagate but do not help to hide the virus
  - UAT (with use cases) is last step in testing process
  - functional requirements specifies the inputs, behaviors, and outputs of software.
  - arrays start counting at 0, so trying to insert an 11th element into array is trying to overflow it.
  - lost updates when one trxn overwrites a value to a database that is needed by trxns that have earlier precedence.
  - TLS is best defense against session hijacking
  - if a system uses shadowed passwords, /etc/passwd would contain x instead of hash.
  - limiting database permissions can help prevent damage from sql injection, but client-side input validation is not useful.
  - Program Evaluation Review Technique (PERT) chart uses nodes, unlike gantt which uses bars.
  - regression testing is performed after devs make changes to an app
  - stealth virus tries to evade virus scans.
  - expert systems need to have knowledge bank and inference engine, neural network is not necessary.
  - checking all input parameters is part of an attack surface identification
  - B? threat modeling often decomposes apps to understand how it interacts
  - polyinstantiation allows storage of different info at different classification levels to stop inference attacks
  - in level 2, the repeatable level of CMM, basic lifecycle management processes

    - atomicity ensures trxns execute complete or not at all.
    - RAD - rapid application development focuses on fast development and only four phases, requirements, user design, construction, and cutover.
- Quiz 9 - Practice test 1
    - NIST 800-53 discusses security control baselines.
    - TGS receives TGT from client and issues a ticket and session key.
    - Asynchronous comms rely on a built in stop and start flag.
    - wave pattern motion detectors will see ultrasonic or microwave signals.
    - stateful packet inspection, aka dynamic, will track state of conversation. Static packet filtering only filter based on source, destination, and ports.
    - DES modes of operation are ECB, CBC, CFB, OFB, and CTR
    - RADIUS is a common AAA protocol. TACACS is cisco proprietary
    - take rule allows a subject to take others rights.
    - Worms will move to uninfected hosts automatically, logic bombs will not.
    - PCI DSS is an industry standard for data security. HIPAA/SOX/FERPA are us laws
    - posting CISSP answers will harm the profession
    - sampling should be done randomly to avoid human bias.
    - US Trusted Foundry ensures supply chain is secure.
    - SAML is used to integrate cloud services.
    - CER, crossover error rate is when the x crosses for type 1 and 2 errors.
    - for the factors of authentication.. factor 4 is somewhere you are, factor 5 is something you do
    - JS is not compiled prior to execution.
    - physical layer deals with electrical impulses as bits
    - Proactive or synthetic monitoring uses recorded or generated traffic to test.
    - one coil inside a card is a proximity card
    - masquerading attacks use stolen or falsified creds to bypass auth. mechanisms.
    - OpenID Connect is an auth layer that works with Oauth 2.0.
    - Parol evidence rule states that when an agreement of two parties is put into written form, it is assumed to be the entire agreement unless amended in writing.
    - SSAE-18 does not assert specific controls and instead reviews the use and application of controls in an externally audited organization.
    - yes privacy shield principles are notice, choice, accountability for onward transfer, security, data integrity, and purpose limitation, access, resource, enforcement, and liability.
    - provisioning through established workflow is workflow-based account provisioning. Discretionary is setting it up for your own stuff.
    - EAL 2 ensures system was structurally tested.
    - During preservation phase a org ensures info related to matter at hand is protected. ID -> Preservation -> collection -> processing
    - Static packet filtering firewalls are known as first-generation firewalls and do not track states.
    - Jitter is variation in latency for different packets.
    - Software tokens are flexible, with delivery options including mobile apps, sms, and phone. Physical tokens are harder to maintain.
    - Yes web apps communicate via web browser interfaces, so interface testing is best.
    - Security Content Automation Protocols handles vulnerabilities and security config info used by NVD by NIST. SCML is not a thing.

    - WBS is a PM tool that divides work done by a large project into smaller components. Project plans discuss timing and resources.
    - Trace coverage is not a type of structural coverage, which are instead like statement, branch or decision coverage, loop coverage, path coverage, and data flow coverage.
    - XST (Cross site tracing) uses HTTP TRACE or TRACK methods to steal a cookie via XSS.
    - limit checks are a type of input validation that ensures data provided to a program are within expected ranges. Buffer bounds are not a thing.
- Quiz 10 - practice test 2
    - rpo is how much data you can lose
    - router should be used to control traffic if protocol is not changed
    - Crystal box pen testing is synonymous with white
    - fingerprinting with web browser is a good automated solution to gather data
    - data owner classifies info
    - SDN allows virtualization for networks
    - Packets leaving network to internet should have source of public ip.
    - developers not able to push code to prod server is separation of duties
    - DoS attacks against VoIP OS is common
    - high priv accounts are typically assessed
    - IaaS gives most control to users, TaaS is not a cloud service model
    - hearsay rule says a witness cannot testify about something they heard.
    - Vendor is providing object based storage, or core infrastructure so IaaS
    - integrity verification helps protect from data diddling attacks from insiders
    - frame relay supports multiple pvcs unlike x.25
    - soc 2 is most detailed report for migration
    - sas 70 was replaced by ssae 16
    - bus and ring can be deployed as star
    - algorithmic complexity is a technique to exploit timing vulnerability.
    - severity level are settings for syslog
    - app level gateway firewall uses multiple proxy servers that filters traffic
    - surveys, interviews and audits measure awareness. Attack surface requires both tech and admin review
    - Multitasking is multiple processes on one processor. Multiprocessing is multiple processes on multiple processors. Multiprogramming needs modifications to apps.
    - When something doesn't work and you put a control in place, it's a compensatory control, even if it is actually another type of control
    - Using encryption lowers likelihood not impact
    - n(n-1)/2 is the formula for sym keys
    - sanitizing includes removing hdd. Purging is more about making die the data is unrecoverable
    - reporting phase of IR notifies law enforcement and regulators
    - bastion hosts can just be very secure hosts.
    - detecting issues is by using Siem, more than just collecting logs
    - l2tp natively supports non IP protocols
    - ER guidelines should have immediate next steps for emergency.
    - triple DES functions need two or three encryption keys
    - APIPA are last /15 in 169, for automatic provisioning of IP when no info is available
    - patching roof is example of physical hardening
    - land attack uses identical source and destination

    - ldap is an open protocol
    - create is a rule in take-grant model
    - EAL7 is formally verified, tested, designed
    - x509 related to certs. X500 is directory services.
    - COPPA is Children's Online Privacy Protection Rule , CCPA is California Consumer Privacy Act
    - Access control systems rely on id and authentication
    - EAP was intended for physical, has no encryption. Peap does though
- Quiz 11 - PT 3
    - NIST SP 800-18 describes system owner responsibilities related to controls, custodian enforces these controls.
    - software quality management occurs in managed state of CMM.
    - Key Risk Indicators (KRIs) are used for ongoing risk management programs.
    - Testing for desired functionality is use case testing.
    - linux tool dd creates a bit-by-bit copy of the target drive, used for forensics
    - yagi and parabolic antennas are directional antenna
    - permissions are access and actions. Rights are actions not access, privileges include both.
    - CWR and ECE (congestion window reduced and ECN-Echo) are rarely used today
    - business or mission owner's role is ensure systems provide value.
    - Electronic Communications Privacy Act (ECPA) makes it a crime to invade electronic privacy.
    - kernel is ring 0, apps at 3, ring 1 is os components, 2 is drivers and protocols.
    - CVSS is the common vulnerability scoring system.
    - Max lengths from shortest to longest: Cat 5e - 300ft. Coax (RG-58) 500ft. Fiber Optic 1000+ ft.
    - Serious dmg = secret. Grave dmg = top secret. Confidental = dmg
    - digital cert provides authenticated copy of sender's public key.
    - Yes last step of cert creation is to sign with CA private key.
    - TKIP was used with WPA to replace WEP. Now CCMP and 802.1x replaced TKIP
    - attribute based info control systems grant authorization by things like identity, department, working hours, etc.
    - certs can only be added to CRL by CA
    - remote journaling transfers trxn logs to remote site more often than electronic vaulting, usually hourly.
    - waiting state is when process is blocked waiting for external event. Ready is for internal blocks.
    - operational investigations are performed by internal teams to troubleshoot, less rigid than criminal, civil, or regulatory.
    - adding second factor can reduce FAR.
    - SOC1 type1 - report that provides auditors opinions of financial statements about controls including presentation of system and suitability of controls. SOC1 type 2 - assessment of material misstatements of financial statement, test of controls, results of tests. SOC2 - benchmarks for controls involving confidentiality, integrity, privacy, availability and information it contains, for restricted use. SOC3- general use report on controls related to compliance or ops.
    - Ide forcing is an integrated development environment and not a type of code review
    - Syslog uses port 514, tcp syslog is 6514. 515 is LPD print and 445 is SMB
    - PSH is a TCP flag to clear buffer, and URG is tcp urgent flag
    - A detection is when you are doing prelim. Triaging.
    - root cause analysis is in remediation step

- business logic errors are missed by automated functional testing
- test coverage = use cases tested / total number of use cases
- callback verifies a phone number is preauthorized.
- iris scans have a longer useful life than other bio factors as they don't change as often
- GLBA is a civil law that requires financial institutions to share and protect customers data. CFAA, ECPA (restrictions on wire taps), and ITADA are criminal laws.
- S/MIME uses P7S format for encrypted email
- Aggregation is a security issue that occurs when a collection has a higher classification than any individual fact. Inference is more about pulling together facts from multiple less sensitive sources.
- Foreign keys are not necessary if there are no other tables.
- foreign keys are used to create relationships between tables (refential integrity
- NIST 800-53 has the examine, interview, and testing processes. Only examine and testing apply to mechanisms.
- Credential management systems provide features designed to make using and storing secure

- Quiz 12 - PT 4
  - COBIT has 5 principles: meeting stakeholder needs, covering enterprise e2e, applying single integrated framework, enabling a holistic approach, and separating governance from mgmt..
  - specifications are document-based artifacts like policies or designs.
  - DevOps process integrates development, operations, and quality assurance and eliminates "throwing problems over the fence" issues.
  - data centers should be located in the core of a building.. Not lower or top floor.
  - due care principle states that individuals should respond reasonably
  - differential backups do not alter the archive bit on a file.
  - OSPF is link state.
  - Machine languages are examples of first-generation programming languages
  - if it is modifiable it is readable, therefore it is subject to tampering and info disclosure based on stride
  - AH as part of IPSec provides auth, integrity, and nonrepudiation. ESP is just encryption and limited auth.
  - digitally signing messages is needed for integrity, hashing alone is not enough.
  - synchronous comms use a timing or clock mechanism.
  - main function of forensic drive controller is to prevent commands from modifying data, aka write blockers.
  - MAC applies to subjects and objects and labels matching.
  - eavesdropping, DOS and caller ID spoofing are common VoIP attacks.
  - TACACS+ uses tcp and encrypts entire session, unlike radius which only encrypts password and uses udp
  - client sends valid TGT to Key Distribution Center (KDC)to request access
  - Cognitive passwords are series of questions that someone knows, like whats your favorite food
  - CDMA GSM and IDEN are 2G. EDGE, DECT, UTMS are 3G. WiMAX LTE and IEE 802.20 are 4G.
  - dry pipe, deluge, and preaction all use pipes that are dry until system finds a secondary validation. Closed-head does not.
  - System owners need to ensure systems are properly labeled and security controls are in place

- Vendors complete security targets (STs) to describe controls. Reviewers compare those to the Protection Profile (PP) to determine if product meets controls.
- United states code (USC) contains all text for laws
- Post-admission philosophy allows or denies access after connection.
- kernel of operating system contains TCB and reference monitor
- fiber optic cables are more expensive but not suspectable to EM interference
- config control ensures software versions are changed in accordance with change control.
- OCSP (Online Certificate Status Protocl) validates certificates in real time
- static code analysis uses techniques like control flow graphs, lexical analysis, and data flow to assess code without running it
- LDAP Bind authenticates and specifies ldap protocol version.
- SDLC includes steps to provide operational training for support staff.
- TCP headers can be 20 to 60 bytes long depending on options
- NIST 800-53 describes depth and coverage.
- XSS filter evasion can avoid just having <script> eliminated
- HIPPA requires anyone working with PHI be subject to a business associates agreement
- transport layer is segments or datagrams (tcp and udp respectively)
- AES is 128, 192, or 256 bit keys
- PGP uses web of trust. RSA, IDEA, and MD5.

- Boson exam 1 - 67%
  - Electronic code book (ECB) DES Mode can leave patterns in ciphertext and is weakest DES mode.
  - Fraggle uses UDP echos
  - Add more disk space is best solution rather than moving to cloud as it is difficult to secure
  - Lipner security architecture combines elements of bell lapadula and biba.
  - DNSSEC can mitigate pharming attacks, which attempt to modify a DNS cache by providing invalid info to DNS server.
  - US Privacy Act made to provide citizens with access to private info being collected by govt.
  - ARP resolves ip addresses to MACs (think what dns does, it gives you an ip)
  - Element of Delay is most likely to involve the most layers of perimeter security defenses
  - Example of encapsulation is when segments are encapsulated in packets, takes a higher layer and adds a header to it.
  - CPU uses four stage pipeline: fetch, decode, execute, and write.
  - Cryptography is not used to isolate subjects and objects from each other (think memory isolation).
  - Pen testers do not need to erase all steps taken to exploit known vulnerabilities
  - Lifetime limits can limit replay attack for keberos.
  - Data custodian backs up company data.
  - Bluetooth uses a weak encryption cipher.
  - KDC enables SSO by acting as a trusted third party auth server. KDC sends TGT and session key. TGS sends ST and second session key.
  - Warm sites can be brought up within 1-3 days. Cold sites are several days or weeks.
  - 5 rules of evidence: Be authentic, accurate, complete, convincing, admissible.
  - Brute force attacker will have access to ciphertext when talking about cryptology.
  - Order of code of ethics goes Protect society, act honorably, provide diligent service, and advance profession.
  - DNS servers typically use a hierarchical database.
  - Vigenere cipher uses a square matrix to encrypt text.

    - Polyinstantiation enables two objects to process data differently.
    - Corrective access control is using AV.
    - Oauth was defined in RFC 6749, not OASIS
    - Circuit-switched wan is best for dedicated lines like T1.
    - Keypad combo locks are most vulnerable to shoulder surfing and brute force
    - MS17-010 is a microsoft identifier. CVE is MITRE
    - SFTP is ssh file transfer protocol…
    - Security markings reflect applicable laws, directives, policies, regulations, and standards.
    - TFTP will use a udp port higher than 1023 generated by the client to send response back.
    - Proxy logs are most likely to contain info about visited websites.
    - Noninterference model can help avoid covert channels. Chinese model is about non-competition. Clark-Wilson use specific programs to access objects.
    - Remote journaling is more about logs and not data.
    - Coupling is dependence on other objects (think of a couple as 2 different people).
    - Standards document would include list of software must be installed.
    - SYN flood occurs at transport layer (TCP)
    - Turnstile can limit only one authenticated person at a time, mantrap does not necessarily do that.
    - Raid 10 uses striping for mirrored. 3 and 4 both use 3 disks and parity.
    - Internet Security Association and Key Management Protocol needs 4 security associations to use IPsec with AH and ESP (two for each).
    - FM-200 is best gas-based suppression system to install in data center.
    - Sensitive data exposure increased in the past few years according to OWASP.
    - Lockdown enclosure prevents theft of computer equipment
    - All firewalls are multi-homed devices (more than one network connection)
    - Flame sensors need line of sight with source of fire
- Boson exam 2 63%
    - Retinal exam is best for small companies with few public visitors cause you can't lose your eyes.
    - Guessing passwords is called a password-guessing, rainbow tables is brute force.
    - Operational controls are executed by people, like ensuring AUP and training. Management controls are focused on risk management and infosec.
    - Salts do not use nonces. Auth protocols, URL requests, and tunneling all use nonces.
    - Fiber optics are least suspectible to unauthorized interception as there is no EM energy.
    - Dedicated High -> system high ->Compartmented -> multilevel (3, 2, 1, 0)
    - TCPIP layers are app, host-host transport, internet, and network access.
    - VMM = hypervisor, VM runs on top of hypervisor
    - DoS can hide a spoofing attack because it can deny the real traffic.
    - Network analysis is most likely to review server logs.
    - OCTAVE (four-phase risk framework) , PUSH (mathematically associates risk events with likelihoods), and NIST SP 800-30 (nine step process) are used to assess risk.
    - ISO 27000, COBIT, and ITIL are for security management best practices.
    - Covert storage channel enables two processes with different security levels to access same info on storage medium
    - System unit contains all internal components of the computer system (the case)
    - Emanation is a threat, which is mitigated through metal conduits protecting UTP cables.
    - Tcp 1024 - 49151 are registered or user ports. 0-1023 are well known or system ports. 49152-65535 are dynamic ports.

- VLAN hopping is primary concern of hosting a VoIP system on same switch as data network
- Most frequently, shared user accounts are for lowering licensing costs or for limited-access resources. Service account is to provide privileges to an app or service.
- Polymorphism allows data to be processed different based on data types when objects are instantiated from other objects.
- FE-13 is safest fire suppressant in electrical environment.
- Warm sites cannot support DR testing as it is not ready without making it a hot site.
- CFB and CBC propagates errors. Worst to best are: ECB, CBC, CFB, OFB, CTR
- Company policy stating that it is not allowed to surf to site is a deterrent access control. Firewall would be preventative.
- Most important consideration of DR is where site is located, at least related to natural disasters.
- CSM/CA is used for 802.11 networks (wireless). Wired use CD.
- Circuit level firewalls operate at layer 5 (session layer). Packet and Stateful operate at 3 and 4.
- Dynamic testing lets you see source code but tests it while running
- Diffie Helmen and ElGamal key exchanges use discrete logaithms.
- 802.11a, g, and n use the OFDM standard.B uses DSSS.
- Red book describes security eval criteria for networked systems. It is a supplement to orange book (TCSEC) which described computer systems.
- Paging is a memory protection technique that copies fixed-length memory to disk. Swapping is copies an entire process to disk. Virtual memory maps hardware memory to applications.
- Avoiding risks would be to cancel implementation of new system. Teaching employees is mitigating risk.
- ISO 27002 is security controls based on best practices. 27001 is about security governance.
- Config management systems use case is hardware asset management (also service modeling, compliance, IR, change impact analysis, change control, event management, and license management).
- PGP can encrypt disk drives but S/MIME cannot.
- SEAL uses a 160 bit key to encrypt. DES uses 566, MD5 uses 128, SHA-1 uis a hashing algo but creates a 160 bit hash.
- Database replication is copying data between live mirrors of a single database.
- Reporting comes before recovery is IR policy.
- When the assessors have a lot of experience they are more likely to perform a quantitative risk assessment.
- Key escrow allows access to sensitive data if the need arises. Recovery agent is for when a key is lost.
- A VPN is mostly likely to be exploited by an internal agent.
- International Associate of Computer Investigative Specialists (IACIS) has several certs related to digital forensics.
- Slack space is unused space in a cluster.
- Any device connected to a promiscuous port is at most a NIDS because it is after the fact.
- Check arp cache if you can't access a computer by its IP address. Hosts file is equivalent to local DNS.
- 80-02.1x says to use EAP to establish port-based communications.
- Transient authentication is something you have. (lasting a short time, think token)
- Damaged mninutiae can cause false rejects in fingerprint readers.
- Multithreading divides cpu time among child processes (aka threads)

- In a BIA you identify critical assets first then do a risk assessment. Recovery strategy is BCP related.
- RIPv1 does not support MD5 auth for secure rote updates.
- API keys can result in unwanted credit card charges as they are often tied to IaaS.
- If company email is on a blacklist ,it is likely that relaying is enabled on the server. Spammers often use open SMTP relays to send spam.
- Electrical charge is used by most smoke sensors to detect fire.
- Remote procedure calls are handed at the session layer. (Also PAP too).
- c-level manager are responsible for developing BCP policy statement.
- Yes Baselining is most likely to monitor security config changes over time.
- Yes Object oriented databases combine data and functions in a code-accessible framework
- Yes Only allocated space is captured during full backup.
- Yes Environmental metric group can be set by end-0user organizations as part of the CVSS.
- Yes anonymization cannot be reverse when implemented properly.
- Yes HTTPS requires sym and asym keys, but s-http does not require aasym keys.
- Yes Bluetooth uses FHSS.
- Yes XACML is most commonly used by SDN systems.

- Boson Exam 3 - 68%
  - A - all of 10.x.x.x, B - 172.16 through 172.31.x.x, C - 192.168.x.x
  - XSRF is least likely to be mitigated via input sanitization
  - Policies should be as short as possible, not contain specifics, should use strong words like must/will.
  - P2PE is point to point encryption but it will not stop external skimmers.
  - CISO would likely not report to internal audit due to conflicts of interest.
  - Boson says "modern ethernet networks" is a star, but Sybex says ethernet is bus.
  - You should not ensure that policy is comprehensive as possible, rather it should be short. The process should be formally defined for creating and maintaining though.
  - Datagrams or segments are sent at layer 4, transport.
  - DNS and DHCP happens at app layer, not network.
  - Kerberos stores secret keys in cleartext.
  - In 802.11 infrastructure mode, clients use AP to communicate with other clients. In client mode, clients only communicate with AP and not other clients.
  - Erasing is the least secure type of data sanitization, equivalent of deleting. Clearing is overwriting. Purging is clearing multiple times.
  - Compensating control is when you implement a solution to support policy.
  - Known plaintext is used if someone has copy of message in both encrypted and plaintext. Chosen plaintext is when you have access to encryption technology and can encrypt plaintext. Chosen ciphertext is when you can choose portions of ciphertext to decrypt.
  - Prudent man rule are business practices that a reasonable individual would consider appropriate.
  - Multitasking enables a cpu to speed processing time by switching from one process to another.
  - Extensible Configuration Checklist Description Format (XCCDF) of the SCAP provides language for specifying security checklists.
  - Elliptical curve is asymmetric so it is less efficient than something like AES.
  - Message Integrity Check is a features of WPA that protects against MitM
  - Pattern-matching means signature matching and they have low false positive rates.

- CSMA requires Acknowledgements of receipt of data, and jam signal is sent whenever data is being sent, and used by devices that cannot send simultaneously.
- National Fire Protection Association standard 75 recommends 60 mins of exposure to fire for tech facilities.
- After SSL handshake, a sym key is used to provide security.
- Diffie hellman is used to exchange keys over unsecure networks.
- Pharming attacks are DNS cache poisoning attacks against DNS servers
- For CVSS, base score affects temporal score, and temporal score affects environmental score.
- Heap metadata protection is a buffer overflow protection mechanism that forces an app to fail if pointer is freed incorrectly.
- EU Privacy principal finality requires data collected to be used for a specific, explicit, and legit purpose.
- Documentation step of change management is most likely to interface with config management.
- Facial scans are often not used for authentication and therefore doesn't need enrollment.
- Side channel attacks are done usually on physical devices like smartcards or crypto devicers using fault analysis, power differential, timing, and emanation attacks to learn info.
- CFTT (Computer forensics tool testing) is a project created by NIST for testing and cert of digital forensics equipment.
- X.400 was replaced by SMTP.
- Decentralized access control requires more admin overhead because it is distributed.
- Mainframe most likely relies on centralized security as all the processing occurs on that unit mostly.
- Teardrop attack sends several large IP fragments and crashes on reassemably (think about trying to combine tears?)
- Minutiae is a term for loops, whorls ridges, and bifurcations found in fingerprints.
- A business is most likely to experience disruptive threats caused by humans.
- Throughput describes the biometric authentication process
- Hybrid security guard system allows you to have control over program and mitigate relationships between guards and employees.
- Physical security controls protect safety of personnel, always primary objective.
- Acceptance phase of SDLC is when it is tested by independent third party.
- Private key is only used for decryption, never encryption of message.
- Ring 0 = 0 kernel, ring 1 = OS components, ring 2 = Device Drivers, ring 3 = user apps and processes.
- Yes, Sherwood Applied Business Security Architecture (SABSA) creates chain of traceability through 6 perspectives of security design.
- Yes, DREAD ranks threats numerically, STRIDE categorizes known threats, PASTA is a risk based threat modeling techinque with stages, Trike uses risk levels for assets.
- Yes, RSN is commonly called WPA2 (Robust security network)
- Yes, ITSEC was influenced by Orange Book (TCSEC). ICC was also but it was also influenced by ITSEC and two others.
- Garbage collection mitigates reuse of info for processors?
- Attack prevention is not a user case for config management systems.
- Transport mode ESP does not encrypt headers, tunnel does. (Think tunnel underground, everything is under.)

    - STP and UTP do not have a copper conductor, just pairs of wire. Coax cables are also shielded.
    - DDoS often utilizes zombies or botnets, which require little or no user interaction to run.
    - Most common work function is the representation of time and effort to perform a successful brute-force.
- Boson exam 4 - 73%!!!
    - RTO is recovery time objective, which is how long it can survive without a service. RPO is recovery point objective, or how much data, measured in time, a business can endure.
    - Zero-day exploit does not need to be newly discovered.
    - Advance and protect the profession includes not developing relationships with those who could harm the profession.
    - TGT enables an authenticated user to access network services. A Session key is encrypted with a client's secret key.
    - Info gathering phase often involves getting a job app form from the client to see what kind of services they run.
    - ActiveX uses digital certs as a security control. Java uses sandboxing.
    - A source IP address is generally not contained in a generic routing encapsulation header (GRC). However, protcol, reserved0, checksum, and reserved1(only if checksum exists) fields can appear.
    - Zero-knowledge testing is blind testing. Blind testing is where the attacker knows nothing, defender may know.
    - System events logs are most likely to show a file deletion. User log would not have the time most likely.
    - Meeting point lead accounts for all personnel after an evacuation. Safety warden just needs to get people out of the building.
    - Virutal memory maps hardware memory addresses to application
    - ::1 is the ipv6 loopback address
    - FF01::1 is ipv6 multicast address
    - During SDLC accreditation, it may be accepted even if it is not certified.
    - Replay attacks are not used to attack RSA, such as man-in-the-middle attacks.
    - VMs with same security requirements are not a threat, but unmanaged ones with different requirements is.
    - A linear cryptanalysis is a known plaintext attack.
    - STRIDE was developed by Microsoft to characterize known threats.
    - PASTA has 7 stages
    - DREAD is to methodology to rank threats numerically.
    - TRIKE allows security audits to be performed consistently, reliably, and repeatably.
    - Security breach means we need to update security policy. New hardware and software doesn't necessarily mean we do, as policies are not technical.
    - You should use live workloads to test software, aka performance testing.
    - SDLC secondary nodes must receive permission from a primary node before transmitting data. HDLC is the upgraded version with error correction and flow control.
    - ITIL was developed by CCTA of UK. TOGAF was developed by The Open Group.
    - US DOD has a requirement of minimum 8 character password, a maximum of 90 days, minimum of 2 days, and history of 24 passwords, with letters, numbers, and symbols.
    - Negative testing is most likely to use boundary tests. Negative testing is the process of issuing invalid information to an application.
    - Barriers are primarily used to delay attackers, not deter them.

- Half-duplex Ethernet uses CSMA/CD. Full duplex does not have collisions.
- P2PE prevents merchants from performing key management, whereas E2EE does not. P2PE encrypts as soon as card is swiped,. Whereas E2EE is decrypted at every step. Both comply with PCI DSS though.
- CHAP periodically reauthenticates users, it is a three way handshake. First step is a random number to the client, then client replies with a hash created using number and shared key, and then third step compares hashes and sends success or fail.
- A business impact analysis should be performed to identify critical systems and processes. BCP is performed when you have already failed.
- You should conduct a BIA right after developing a BCP policy. BCP process: Develop bcp policy, conduct bia, identify preventative controls, develop recovery strategies, develop IT contingency plan, perform DRP training and testing, perform BCP/DRP maintenance.
- A cloud-based deployment solution most likely has the software AND hardware operated and maintained by a third party.
- Object reuse is limited to reusing data or creds in memory or cached on disk.
- A botnet is a network of zombies.
- Background checks are a preventative, detective, and deterrent access control.
- Pointer encoding is a buffer overflow protection mechanism that is recommended but not required for ISV or SDLs. ASLR, Heap Metadata Protection, and DEP are all requirements for SDL.
- MACs are 48 bits long and assigned by the hardware manufacturer.
- Tampering attempts are least likely to produce user-visible messages.
- Use ALE to calculate when it says typically needs to be replaced every x years and add it to purchase cost.
- Lexical obfuscation deals with renaming fields, classes, and methods with shorter ones like salary with a, to make the application smaller.
- Best evidence rule states that courts should be provided with best evidence possible to establish the facts of the case. Relevant, authentic, accurate, complete, and convincing.
- Yes, DRAM uses capacitors to store info and needs constant refreshing. It is slower and cheaper than static access ram.
- Yes, Third nominal form (3NF) describes normalization process of removing data not dependent on primary key. Data normalization process of logically dividing data that depends on primary keys into tables is known as 1NF. Moving data that partly depends on primary keys into a different table is known as 2NF.
- Yes, Enticement is when they were going to commit a crime, entrapment is when they were not.
- Yes, centralized access systems can be a single point of failure. Decentralized access systems define access rules and permissions in a sphere of trust.
- Yes, Abstraction is the process of hiding operational complexity of a system from its users.
- Yes, an iris scan is the most accurate noninvasive biometric access control.
- Yes, a row of data is a tuple in a relational database. A relation is a table.
- Yes, A photoelectric motion sensor emits a beam of light across a path that is monitored.
- Yes, a CSRF/XSRF involves the redirection of static content within a trusted site.
- Yes, typosquatting relies on typos and cybersquatting is the exact name that is trademarked.
- Yes, an asynchronous dynamic password token generates passwords after you enter a pin.
- Yes, a DOS usually a simultaneously occurs with a spoofing attack.
- Yes, Oauth 2.0 was defined in RFC 6749 and based on IETF. 5849 defined Oauth1.0. Oauth is decentralized authorization, OpenID is decentralized authentication.

    - Yes, rights allow you do perform specific actions. Permissions give access. Inheritance is related to groups, explicit is individuals.
    - The X.500 object that contains full path to entry is the DN.
- Boson Quiz 5 - 81%
    - Example of accountability is reviewing a server for logs of malicious activity
    - DNS cache poisoning is least likely to need a MAC spoof. ARP, CAM and DoS related attacks do.
    - Due care is minimum level of info protection that an organization should achieve. Due diligence requires organizations to review its practices.
    - FTP port 20 is for data transfer, port 21 is for control commands.
    - Dense grove of trees infront of a retail building's windows and doors is not good crime prevention through environmental design (CPTED)
    - BCP plan are in the following steps: Develop BCP Policy, Conduct BIA, Identify Preventative Controls, Develop Recovery Strategies, Develop IT Contingency Plan, Perform DRP Training, Perform DRP Maintenance
    - Prevention obfuscation deals with making programs obscure to computers.
    - T1 is a circuit switched WAN technology
    - Encapsulation, aka data hiding, ensures that a class defines only the data that it requires
    - A threat vector is a potential medium that an attacker can use to exploit a vulnerability, like an email that contains an attachment. Careless employee is a threat agent.
    - Cache memory is the fastest type of computer memory and used by the CPU. Register and L1 are both in cpu and L1 is slower, L2 is slower than L1 but is outside CPU.
    - Role based access control is least likely to control access by using explicit rights and permission (because you are not explicitly assigning to an individual).
    - Overt channel is communication that is authorized and performed in compliance with security policies.
    - MD5 creates a 128-bit hash. AES and RC5 do not do hashes, they are block ciphers. SHA-1 creates a 160 bit hash.
    - OpenID connect and OAuth2.0 are both defined in RC6749 but only OpenID connect is not maintained by the IETF.
    - Hardware segmentation maps processes to specific hardware memory locations. Swapping copies processes to disk.
    - Telnet provides neither conditionality nor integrity, even though it is over tcp port 23.
    - Access control mechanisms are most likely to include a reference monitor, as it determines whether a subject with a clearance level can access an object of a different classification level.
    - Security labeling refers to the use of security attributes for internal data structures within information systems. Security marking is human-readable security attirbutes.
    - WS-SecureConversation Web Service Specs create security contexts for faster message exchanges.
    - WS-Security Web Services is for integrity, encryption, and authentication for SOAP messages.
    - TOGAF uses business requirements as a central point of comparison for every phase of development.
    - Vascular patterns are not easy to be counterfeited, but fingerprint scanners are.
    - Legitimately requires that data collected is used in a way that is compliant with a legal requirement or employee's consent. Finality is that data is collected for specific, explicit, and legitimate purpose.

- XSS was not a top 3 of OWASP 2017.
- Piracy is not infringing on trademarks, it is an IP attack on copyright.
- Dilution occurs when an entity uses a trademarked term as a generic term.
- Common Criteria Security Target is the documentation for the system or product that is to be tested. PP is the security requirements and objects for the product to be tested.
- OSPF learns the entire network topology for the area, but does not send periodic routing updates, only when topology changes.
- WPA2 uses CCMP for integrity mode, which uses a message integrity code to validate if it was tampered with. WPA2 uses 802.1x or psk for authentication. AES for encryption. WPA uses TKIP for integrity and RC4 for encryption.
- A Caesar cipher is not a polyalphabetic cipher, it is a monoalphabetic cipher (simple substitution scheme, which is vulnerable for frequency analysis)
- Yes, Using an image of the disk to collect data is most likely to prevent corruption of evidence.
- Yes, Risk density ranks security issues in order to quantify risk.
- Yes, deadlocking happens when two database processes are denied access to a record at the same time
- Yes, Relative Distinguished Name is synonymous with an LDAP CN.
- Yes, compartmentalization ensures info does not flow between groups of users.
- Yes, an extranet is to provide customers with access to the company's network.
- Yes, the ring model is a method of hardware layering that uses system calls to communicate with the CPU.
- Yes, negative testing is just putting invalid input, boundary testing is putting numbers out of bounds, positive testing is putting valid inputs, CRUD is database related.
- Yes, database shadowing requires two databases running simultaneously for backup.
- Yes, port 88 is for Kerberos authentication. IKE is port 500, L2TP uses UDP 1701
- Yes, Zigbee and Bluetooth are all personal area networks.
- Yes, SLIP has been replaced by PPP, can transfer several different network protocols, can use PAP, CHAP, and EAP, and supports sync links like T1 line and async links like dialup.
- Yes, FE80::/10 enables a computer to configure an address for itself.
- Yes, product security certification means system was tested and meets data owner's security reqs.
- Yes, T1 and T3 are mostly located in US, Canada, Japan, and South Korea. E1 and E3 are used elsewhere.
- Yes, SNMPv3 was first to offer both auth and encryption.
- Yes Zero-knowledge testing offers nothing to the pen tester other than what's publicly available.
- Yes, a block cipher best describes DES.
- Yes, MIMO is not supported on WLAN until 802.11n
- Yes, RSA is susceptible to chosen ciphertext attacks.