Study Guide

CISSP

Created By: Dimitrios Taketzis, Teaching Assistant

Module 1: Welcome and Introduction

Lesson 1.1: Introduction

Skills Learned From This Lesson: Security, Risk Management, Overview

- The 8 Domains of CISSP
- 1st Domain -> the most Important
- 2nd Domain -> how to protect my assets
- 3rd Domain -> 2 Chapters, the 1st is Security Architecture and Design + Software development Security and the 2nd is Cryptography
- 4th Domain -> Becoming very popular is exam
- 5th Domain -> Comprehensive look on networking
- 6th Domain -> Testing
- 7th Domain -> redundancy + Continuity of Enterprise
- 8th Domani -> Managing the project of creating Software, not writing code

Lesson 1.2: Computer Adaptive Testing (CAT)

Skills Learned From This Lesson: Test Method, Question Format, Domain Weights

- A new method of testing -> going from 250 questions and six hours of testing to max. 150 questions and three hours
- No. of questions 100 - 150
- Question format -> MCQ and advanced innovative questions
- Passing grade 700 - 1000 points
- Different average weight for each domain
- Cannot mark questions for review anymore
- Risk Mgmt to start -> Business Continuity as our ultimate goal

Lesson 1.3: Domain 1 Agenda

Skills Learned From This Lesson: Security Principles, Security Governance, Security Program, Risk Mgmt

- Principles of Security
- Security Governance (Strategy, Blueprints and Frameworks)
- Information Security Program (Policies, Standards, Procedures, Guidelines, Roles and Responsibilities)
- Information Security Risk Mgmt (Identification,Assessment,Mitigate, Monitoring)
- Legal Consideration
- Knowledge Transfer

Lesson 1.4: Information Security Program Part 1

Skills Learned From This Lesson: Policy Types, Standards, Security Program

- Three types of policy (Why?) (Corporate, System Specific, Issue Specific)
- Standards fill the gaps of policy, they change frequently
- Policies are very broad, not change frequently
- Corporate Policy -> Very broad, Management philosophy and commitment
- System Specific Policy -> eg. Multi factor authentication for system
- Issue Specific Policy -> Nebulous issues that need to be defined so there is no misunderstanding
- Separation of Duties (Segregation of Duties, Separation of Role) -> Really valuable control, it forces collision

Lesson 1.5: Information Security Program Part 2

Skills Learned From This Lesson: Policies, Standards, Procedures, Guidelines, Baselines

- Issue specific Policies (...contd)
- Mandatory Vacations -> Detective control
- Job Rotation ->Detective control and redundancy method
- Least Privilege <-> SOD, action, what can you do
- Need to know <-> SOD, about data, permissions to data
- Dual Control -> Prevent abuse of power
- M of N control -> 4 of 9 must be present to do an action
- Standards (what?) -> Mandatory, support or reinforce policy, provide specific details, directions, can be internal or external

- Procedures (How?) -> Mandatory, step by step directives, detail the how to meet policies, standards and guidelines
- Guidelines -> Not mandatory, suggestive in nature, recommended actions, best practices
- Baselines -> Mandatory, the minimum acceptable security configuration for a system or process, the purpose of security classification is to determine and assign the necessary configuration to protect data

Lesson 1.6: Roles and Responsibilities

Skills Learned From This Lesson: Security Roles, Responsibilities, Duties

- Senior Mgmt Responsibilities -> Provide oversight, funding, support, ensure testing, prioritize business functions, establish vision, strategy for the enterprise, sign off on policy and Business Impact Analysis
- Steering Committee -> oversight of Infosec Program, Liaison between Mgmt, business, Info Technology and Info Sec, Into the decision making process, compliance
- CISO-> Strategic Planning, Policy Development, Tech Assessments, Process Improvement, Acquisition, Capital Planning, Security
- Info Sec Manager-> Responsible for determining the how, introduces methodology, major consultant of senior mgmt
- Business Managers -> customers, responsible for business ops, security enforcement and operation, day-to-day monitoring, reporting, disciplinary actions and compliance
- Security Practitioners-> responsible for proper implementation of sec requirements in their IT systems, identify and assess new potential risk and implement new security controls to safeguard IT systems
- Auditors-> ensure that controls and policies are implemented and they are effective through Objective Evaluation, they only document, not modify
- Security Trainers->must understand risk mgmt process, training materials, awareness programs, incorporate risk assessment to training programs, encourage users to report violations
-

Lesson 1.7: Risk Definitions

Skills Learned From This Lesson: Risk definitions, Risk Mgmt, Security measures

- Information Security Risk Mgmt

- Asset, Vulnerability, Threat, threat agent, exploit, risk, controls (physical, administrative, technical protections), total risk, residual risk, secondary risk
- Safeguards -> proactive measures, prevent, deter
- Countermeasure -> reactive measure
- Incident-> a risk event that has transpired
-

Lesson 1.8: Risk Identification

Skills Learned From This Lesson: Risk identification, Risk mgmt, Defense lines

- Risk mgmt steps (identification, assessment, mitigation/response, ongoing controls evaluation)
- Risk identification process
- Methods to identify risks (sources of risk documentation, audit reports, incident reports, interview with SMEs public media, annual reports, press releases, vuln assessments and penetration tests, threat intel services)
- Alignment with Business Goals and Objectives -> understand business strategy, meet with mgmt to support you, look beyond IT
- Organizational Structures and Impact on Risk -> risk context, risk mgmt approach should be enterprise wide
- Three lines of defense -> business units(perform the work day-to-day), risk and compliance (guidance and direction), audit (review 1st and 2nd lines)
-

Lesson 1.9: Risk Assessment and Analysis

Skills Learned From This Lesson: Risk Analysis, Qualitative, Quantitative

- Qualitative risk assessment/analysis -> subjective analysis to help prioritize and impact of risk events (eg. Delphi Technique)
- Probability and impact Matrix -> subjective input, high, medium, low terms and it is a quick way to begin the prioritization and ranking of risks
- Quantitative risk assessment/analysis provides a dollar value to a particular risk event
- Quantitative requires more experience than Qualitative
- Quantitative analysis allows for good business decisions, provides justification for a mitigation strategy
- Asset Value, Exposure Factor, Single Loss Expectancy, Annual Rate of Occurrence, Annual Loss Expectancy, Total Cost of Expectancy, Return of Investment

- I am looking a way to implement a control that has a positive return of investment, that mitigates a risk to my business to a degree that is acceptable by senior mgmt
-

Lesson 1.10: Risk Mitigation and Response

Skills Learned From This Lesson: Risk mitigation, Risk response , Response means

- Steps for Quantitative Analysis
- AV -> EF -> SLE -> ARO -> ALE -> Perform cost/benefit analysis of countermeasures
- Risk response means (Reduce, Avoidance, Transfer, Accept, Rejection)
- Risk reduction/avoidance -> action taken to lessen the frequency and/or impact of a risk, the ultimate risk reduction is avoidance (risk is 0)
- Risk elimination is unfeasible
- Risk transference is a decision to reduce loss through sharing risk with another organization (SLA and contracts establish the degree of transference)
- Risk acceptance -> no active mitigation, based on cost/benefit analysis it is determined the cost of control is less than loss
- Sometimes acceptance is the only choice and includes due diligence, regular reviews are needed because level of risk and impact is always changing
- Risk acceptance is different from risk rejection (no liability)
- Risk rejection is unacceptable
- Whatever our risk is, we will mitigate until my residual risk falls within the acceptable level
-

Lesson 1.11: Risk Monitoring and reporting

Skills Learned From This Lesson: Risk monitoring, Risk reporting, KRIs

- How often should we go back and reevaluate our controls?
- Risk monitoring is an essential step of the risk mgmt life cycle because of the changing nature of risk and associated controls
- Key Risk Indicators (KRI) is a warning sign, they provide a backward-looking view on risk events, increase the likelihood of achieving strategic objectives
- Examples of KRIs -> quantity of unauthorized equipment or software detected,
- KRIs support -> risk appetite, identification, mitigation, culture, measurement and reporting, compliance
- Risk mgmt Process Review (the four steps)
- Risk cannot be totally eliminated, so it must be managed

-

Lesson 1.12: Legal Considerations

Skills Learned From This Lesson: Legal Considerations, Law types, Legal Liabilities

- Liabilities -who is at fault?
- Failure of Mgmt to execute Due Care and/or Due Diligence can be termed negligence
- Due Diligence -> eg. researching industry standards and best practices
- Due Care -> eg. setting and enforcing policy to bring organization into compliance
- Downstream Liabilities -> i can outsource work but i cannot outsource liability
- Types of laws -> criminal, civil, regulatory, Intellectual Property
- Criminal law -> beyond a reasonable doubt, which can be difficult to meet in computer related crimes
- Goal of criminal penalties is 1) punishment 2)Deterrence
- Civil (Tort) law -> preponderance (predominance) of evidence
- Administrative (regulatory) law -> defines standards of performance and regulates conduct for specific industries
- Intellectual property law -> protects properties of mind,
- WIPO investigates and pursues copyright violations
- Licensing is the most prevalent violation, followed by plagiarism, piracy and corporate espionage
- Trade secret -> gives value to a company (secret recipe), must be genuine and not obvious
-

Lesson 1.14: Knowledge Transfer

Skills Learned From This Lesson: Knowledge Transfer, Security Awareness, Training Benefits

- Knowledge Transfer -> Awareness, Training, Education ->the goal is to modify behavior
- Security awareness training must fit job description
- Knowledge transfer benefits -> modify behavior, improves attitudes towards info sec, accountability, raises collective security awareness level of organization
- Wrap up of Domain 1
-

Lesson 1.15: The CISSP Mindset Part 1

Skills Learned From This Lesson: CISSP approach, CISSP Mindset,

- I am a risk advisor - I do NOT fix problems
- Who is accountable for security ? -> Everyone

- How much security is enough ? Just enough is enough, a good risk mgmt will drive my decisions, efficient use of resources
- Everything starts with risk mgmt
-

Lesson 1.16: The CISSP Mindset Part 2

Skills Learned From This Lesson: CISSP approach, CISSP Mindset

- Think “End Game” -> which answer truly satisfies the question??
- Security transcends Technology -> Security must be based on good foundational principles, it is bigger than technology
- The answers are not too technical or too managerial, they are in the middle
- Incorporate security into the design, as opposed to adding it later
- Layered defense! -> No one device will keep you safe
-

Lesson 1.17: Introduction to Business Continuity and Disaster Recovery Planning

Skills Learned From This Lesson: Business Continuity*, Disaster Recovery, incident response*

- Minimize impact on business
- Incident Response -> forensics, investigating in a manner that can be presented in a court of law
- Redundancy -> it has to be comprehensive
-

Lesson 1.18: Business Continuity Planning Part 1

Skills Learned From This Lesson: Business Continuity*, Disaster Recovery, Disruption Categories*

- BCP -> focuses on business, sustain operations and protect viability of the business following a disaster, umbrella term that includes many other plans, long term focused
- DRP -> focuses on IT systems, minimize effects of a disaster, take steps to ensure that resources, personnel and business are able to resume in a timely manner, short term focused
- BCP Relationship to Risk Mgmt -> BCP is the safety net to RM, RM is “if then”, BCP is “whatever” (didn't see that coming->but I have a plan)
- Categories of Disruptions (Non-disaster, emergency/crisis, disaster, catastrophe)
- Incident is a non-disaster
- Emergency/Crisis -> urgent event where there is the potential for loss of life or property

- Disaster -> facility unusable for a day or longer, normal operation are halted, DRP 1st phase (notify)
- Catastrophe -> destroy facility
- BCP coordinator can only declare a disaster
-

Lesson 1.19: Business Continuity Planning Part 2
Skills Learned From This Lesson: Business Continuity*, NIST framework, ISC2 framework*

- BCP Frameworks (DRII, NIST 800-34 rev 1, ISO 27031, BCI GPG, ISC2.org four processes of Business Continuity)
- Don't stick to the terms, stick to the concept and flow
- Standards help solve issues of inconsistency in terms
- NIST 800-34 rev1 -> 7 phases -> BCP Policy, Business Impact Analysis, Identify Preventive Controls, Create Contingency Strategies, Develop an IS Contingency Plan, Testing-training-exercises, maintain BCP
- ISC2 four BCP processes -> Project scope and planning, Business Impact Assessment, Continuity planning, Approval and implementation
-

Lesson 1.20: BCP Step 1: Project Scope and Planning Part 1
Skills Learned From This Lesson: BCP Plan, BCP Methodology, Project Scope

- Step 1 -> - Acquire BCP Policy Statement from Senior mgmt
- - Business Organization Analysis : Structured analysis of the business organizational assets, it provides the groundwork necessary to help identify potential members of the BCP team and the foundation for the remainder of the BCP processes, evaluates operational departments that are responsible for the core services, critical support services, senior executives and other key individuals essential for the ongoing viability of the organization
- - BCP Team Creation, including Project Manager -> cross-functional, including representation of senior mgmt, from each department, IT with technical expertise in areas covered by BCP
- - Assessment of resources available and commitment to support the BCP Process from Senior mgmt for Development, Testing-training-maintenance and Implementation
- - analysis of legal and regulatory landscape iot operate within a legal framework during an event. Senior mgmt has the ultimate legal responsibility

-

Lesson 1.21: BCP Step 1: Project Scope and Planning Part 2
Skills Learned From This Lesson: BCP Plan, BCP Methodology, Project Scope

- BCP Regulation Examples (Healthcare, Government, Finance)
- Usually, people understand very little the importance of BCP, they only want to be compliant
-

Lesson 1.22: BCP Step 2: Business Impact Assessment Part 1
Skills Learned From This Lesson: BIA Assessment, MTD/MTO, RTO

- BIA -> identifies and prioritizes all business process/resources based on the criticality (MTD/MTO, RTO [less than MTD and not only to obtain the hardware but to also restore its services], RPO [data loss tolerance])
- Risk Identification
- Categorized processes/resources based on criticality
- Defines quantitive metrics to assist with prioritizing recovery focus
- BIA help prioritize recovery priorities
-

Lesson 1.23: BCP Step 2: Business Impact Assessment Part 2
Skills Learned From This Lesson: BIA Assessment, Cloud Risk, Risk Probability

- Critical Resources identification
- Step 2: BIA: Risk Associated with Procurements and the Cloud
    - Evaluate CSP's BCP -> Examine SLA
    - Verify Controls in place to meet obligations in person or SOC -> Service Organizational Controls
    - SOC 1 -> financial
    - SOC 2 -> Security and Technology
    - SOC 3-> Security and Technology publicly available
- BIA: Probability and Impact Assessment
    - Total risk
    - Residual risk
    - AV
    - ARO
    - Impact EF
    - SLE

    - ALE

- BIA: Resource Prioritization
    - Qualitative Analysis
    - Quantitive Analysis

Lesson 1.24: BCP Steps 3 and 4: Continuity Planning, Approval and Implementation
Skills Learned From This Lesson: Continuity Planning*, BCP Approval, BCP* Implementation

- Step 3 -> Examines BIA and maps controls to meet the objectives
    - Determine responses (reduce, assign, accept, reject)
    - Some risks are accepted while others require a more active strategy
- Continuity Planning: Provisions and Processes
    - 3 assets (People -> 1st Priority, facilities -> hardening provisions, alternate sites [mirrored, leased, cold, warm, hot], Infra)
    - Cold Site -> only building, weeks to operate
    - Warm Site -> furniture, equipment, basic infra, connectivity -> days/hours to operate
    - Hot Site -> ready to operate, expensive, exclusive use, MOA/MOU from the provider (because its a leased facility) -> hours/minutes to operate
    - Infrastructure -> supports the critical elements of the business, servers, systems, routers, switches, processes, architecture
    - High availability (redundancy, resiliency, fault tolerance)
    - mirrored site (belongs to the organization)
    - Cloud changes this overall approach
- Step 4: Plan Approval and Implementation
    - Approval ->CEO or Senior Officer, indicate dedication of the business to the BCP
    - Implement -> Create guide, deploy resources, supervise
    - Train and Educate employees -> distribute plan on need to know basis, everyone an overview
-

Lesson 1.25: BCP Sub Plans
Skills Learned From This Lesson: BCP Plans, Plan Roles, Plan Responsibilities

- Sub-plans of BCP have 3 purposes -> **Protect** (Crisis Communication Plan, Occupant Emergency Plan), **Recover** (Business Recovery Plan, Disaster Recovery Plan,

Continuity of Support Plan/IT Contingency Plan), **Sustain** (Continuity of Operations Plan)
- CCP -> disseminate necessary info
- OEP -> minimize loss of life and protect property damage in response to physical threat
- BRP -> provide procedures for recovering business operations after a disaster
- CSP/IT CP -> provide procedures for recovering a major application or general support system
- Cyber Incident Response Plan -> Provide strategies against cyber incidents
- DRP -> Provide procedures to facilitate recovery of capabilities
- COOP -> Provide procedures and capabilities to sustain an organization's essential strategic functions at an alternate site for up to 30 days, not IT focused, in NIST its a part of BCP not instead of BCP
- Roles and Responsibilities ->
    - **Senior Executive Management** (approval and support of plans, setting continuity policy, prioritize critical functions, allocate resources, approves BCP, review test results, ensures maintenance of a current plan)
    - **Senior Functional Management** (develop and document maintenance and testing strategy, identify and prioritize mission-critical systems, monitors progress of plan development and execution, tests, creates teams to execute plans)
    - **BCP Steering Committee** -> Conducts the BIA, coordinates with department representatives, includes Business units, senior mgmt, IT, Security, Communications, Legal
    - **DRP teams** -> rescue (deal with the immediacy of disaster), recovery-failover (getting the alternate facility up and running and restore the most critical services first), salvage (return of operations to the original or permanent facility)
-

Lesson 1.26: Developing the Teams

Skills Learned From This Lesson: Team Development, Media Communications, Team Responsibilities

- Who will talk to the media? Somebody who is trained to do so, not necessarily the CEO
- Who will setup alternative communication methods?
- Who will setup the offsite facility?
- Who will work on the primary facility?
-

Lesson 1.27: Types of Tests
Skills Learned From This Lesson: Test Types, Post-Incident Review, Maintain BCP

- Checklist test -> Copies of plan distributed to different departments
- Structured walk-through (tabletop) test -> representatives from each department go over the plan
- Simulation test -> going through disaster scenario
- Parallel test -> systems move to an alternate site
- Full Interruption test -> original site shut down, all of the processing moved to offsite facility

- Post-incident review -> focus on how to improve, what should have happened, what should happen next, not who's fault it was (unproductive)

- Maintaining the BCP -> keep plan in date -> make it a part of business meetings and decisions, centralize responsibility for updates, part of job description, Personnel evaluations, report regularly, Audits

Module 2: Asset Security

Lesson 2.1: Introduction to Asset Security
Skills Learned From This Lesson: Asset Security*, Asset Value, Asset Classification*

- Agenda -> Asset Value and Classification
    - Data Protection
    - Data Redundancy
    - Secure Data Disposal

Lesson 2.2: Data Classification
Skills Learned From This Lesson: Data Classification*, Asset Value,* Sensitivity and criticality

- What makes up the value of an asset? -> value to the organization, loss if compromised, legislative drivers, liabilities, value to the competitors, acquisition costs,
- Data classification -> sensitivity labels for data for the purpose of configuring baseline security based on value of data
    - Cost -> value of the data

    - Classify -> criteria for classification
    - Controls -> determine the baseline sec config for each
    - Data owner -> determines the classification of data
    - Data custodian -> maintains the data

- Both government and private sector use data classifications
- Sensitivity vs criticality -> Sensitivity describes the amount of damage that would be done should the information be disclosed and affects confidentiality, Criticality describes the time sensitivity of the data and affects availability
-

Lesson 2.3: Data Protection

Skills Learned From This Lesson: Data Protection*, Data States, Integrated Security*

- **Location?** Where is the data stored/processed/ transmitted -> jurisdiction, audit, threat landscape, what actors have access to the data, does data move between locations and how?
- **Access** -> Who has access to the data? What controls are in place? what devices can be used to access data?
- States of Data -> At rest (File System Encryption, EFS, TPM), In Process, In Transit (SSL/TLS)
- Hardware-based encryption -> encrypts the entire drive and not only file system to avoid mounting drive to another operating system and read data, BitLocker, Trusted Platform Module (TPM)
- What security is built-in in IPV4? Nothing, so we encapsulate inside another packet like IPSec, IPV6 is integrated in IPSec so it includes security
-

Lesson 2.4: System Hardening and Baselining

Skills Learned From This Lesson: System Hardening*,* System Baselining*,*

- Hardening -> remove unnecessary services, install the latest services and patches, rename default accounts, change default settings, enable auditing-firewalls-updates, physical security!!
- Windows OS was easy to use -> big attack surface -> the opposite of security
- Remove unnecessary services through change requests (change control) because I may use it but not know it
-

Lesson 2.5: Threats to Data Storage

Skills Learned From This Lesson: Data Threats, Cloud security, DRM

- Unauthorized usage/access (Strong auth, encryption, obfuscation, anonymization, tokenization, masking, policies, layered defense)
- Liability due to noncompliance (due care and due diligence, SLAs)
- DoS and DDoS (redundancy, data dispersion)
- Corruption, modification, destruction of data (hashes/digitally signed files)
- Data leakage and breaches (DLP)
- Theft or accidental media loss (TPM)
- Malware attack (anti-malware)
- Improper treatment or sanitization of data at the end of life cycle

Data Security in the Cloud

- Protect data moving to and within the cloud (SSL/TLS/IPSec)
- Protect data in the cloud (encryption)
- Detection of Data Migration to the Cloud (DAM[Database Activity Monitor]. DLP)
- Data dispersion -> data is replicated in multiple physical locations across your cloud. Is used for higher availability
- Data fragmentation -> splitting a data set into smaller fragments (or shards) and distribute them across a large number of machines

Data Loss Prevention -> or Data Leakage Prevention = controls put in place to ensure certain types of data (SSNs, Account Numbers) remain under organization controls in line with policies, standards and procedures, detects exfiltration of certain types of data, help compliance with HIPAA,PCI-DSS and others

- Obfuscation -> process of hiding, replacing or omitting sensitive information
- Masking -> use specific characters to hide certain parts of a specific dataset
- Data anonymization -> the process of encrypting or removing PII from datasets, so that people whom the data describe remain anonymous
- Tokenization -> its like a shortcut, not giving direct access to the data but a token IOT protect the data, eg. public cloud service can be integrated and paired with a private cloud that stores sensitive data. The data sent to the public cloud is altered and contains a reference to the data residing in the private cloud

- Data rights management -> DRM or IRM adds an extra layer of access controls on top of the data object or document and provides granularity flowing down to printing, saving, copying and other options, protects sensitive content and intellectual property, ACLs that are embedded into the file and travel with the file (persistent)
-

Lesson 2.6: Data Redundancy

Skills Learned From This Lesson: Data Redundancy, Cloud Considerations, Data archiving

- Backups and Archives -> what we backup, how often, where, how long
- BIA -> which services are the most important
- RTO -> Recovery Time Objective, how quickly I have to restore it
- RPO -> Recovery Point Objective, how current the data must be
- Data Retention -> protocol for keeping info for operational or regulatory compliance needs
- Cloud Considerations -> legal, regulatory and standards requirements must be well documented, data mapping, data classification
- Data archiving -> identify and move inactive data out of current productions systems into specialized long-term archival storage systems and includes encryption granular retrieval, e-discovery, backup, media type, restoration procedures
- S

Lesson 2.7: Secure Data Disposal

Skills Learned From This Lesson: Data Disposal, Sanitization, Data Remnants

- Sanitizing Media -> types, size of media storage needed
- Confidentiality of data stored in the media
- Will the media be processed in a controlled area?
- Should the sanitization process be conducted within the organization or outsourced?
- What is the anticipated volume of media to be sanitized by type of media?
- What is the availability of sanitization equipment and tools?
- Deleting or formatting is not the right answer!!
- If you are going to reuse the media ->zeroization
- If you are not going to reuse the media -> physical destruction
- Degaussing is in the middle
- Clearing-overwriting -> renders data inaccessible by normal means
- Purging-degaussing -> renders media unusable by normal means

- Destruction-physical destruction -> irreversible by all known techniques

Module 3: Security Engineering and Architecture

Lesson 3.1: Cryptography Agenda

Skills Learned From This Lesson: Cryptography Agenda*, Introduction, Module Description*

- Very testable

Lesson 3.2: Cryptography in History

Skills Learned From This Lesson: Cryptography in History*, Caesar cipher, Enigma/Purple Machine*

- Caesar Cipher *, Scytale, Vignere, Vernam *, Enigma * and Purple Machine (*focus on these)
- Caesar -> simple substitution, shift characters 3 spaces, A=D, B=E, C=F etc. , substitution ciphers are subject to pattern analysis, ROT 13
- Scytale -> spartans used it, wrapped tape around a rod, the diameter of the rod is the pre-agreed upon secret
- Vignere -> first polyalphabetic cipher, a keyword is agreed upon ahead of time, the first letter of the key is matched up against first letter of the message and so on
- Enigma/Purple machine, added complexity, a secret is shared between the two parties out of band
- Vernam cipher -> one time pad, the only mathematically unbreakable form of cryptography, key must be used only once, pad must be at least as long as the message, key pad is statistically unpredictable, key pad must be delivered and stored securely
-

Lesson 3.3: Security Services Provided by Cryptography

Skills Learned From This Lesson: Cryptography Services*,* Cryptography Definitions*, Initialization Vector*

- Cryptography Services -> Privacy, Authenticity, Integrity, Non-repudiation (authenticity + integrity)
- Plain text + IV + Algorithm (Cipher) + Key = Cipher Text

- Initialization Vector -> randomize the starting point of a process, used for confidentiality similar to a ”seed” (at the beginning of the process) or “salt” (at the end of process) for password protection
-

Lesson 3.4: Algorithm

Skills Learned From This Lesson: Algorithm, *Keys, Algorithm qualities*

- Algorithm -> a collection of math functions that can be performed
- Keys -> how to use the math
- Qualities of an Algorithm -> Confusion, Diffusion, Avalanche, Permutation, Open-Kerchhoff’s Principle
- Confusion -> complex substitution, strong math
- Diffusion -> getting more complexity by combining plaintext and ciphertext
- Avalanche (chaining) -> when output from one function provides input to the next
-

Lesson 3.5: Elements of Cryptography Part 1

Skills Learned From This Lesson: Permutation, Open-Kerchhoff’s Principle*, key qualities*

- Permutation -> the idea of rounds
- Open-Kerchhoff’s Principle -> openness in the algorithm, the key is secret, US government does not agree with this and keeps both closed
- Security through obscurity -> by hiding it, it cant be broken
- GO open for the purpose of the test
- Key qualities -> long, random, secret
-

Lesson 3.6: Elements of Cryptography Part 2

Skills Learned From This Lesson: Symmetric Cryptography, *Stream Ciphers, Block Ciphers*

- Symmetric -> stream (RC-4 only!), Block (AES/3DES)
- Asymmetric -> Discrete logarithms (Diffie-Hellman, ECC, El Gamal), Factorization (RSA)
- Symmetric -> efficient, the most common, much faster than asymmetric
- Stream ciphers are weaker than block ciphers but very fast
-

Lesson 3.7: Principles of Secure Design

Skills Learned From This Lesson: Skill, Skill, Skill

- Security model -> lays out the framework and mathematical models that act as security-related specs for a system architecture, it is a concept

- System architecture -> the overall design of the components such as hardware, OS, applications and networks - of an information system, brings the model to life
- State Machine Model -> if a system starts securely and functions and shutdowns (or crashes) securely it is a secure system
- The startup of a system is the most difficult because the security mechanisms have not loaded yet
- During shutdown (trusted recovery) -> in the event of a violation the system should terminate with no further compromise
-

Lesson 3.8: Security Models Part 1

Skills Learned From This Lesson: Security Models, Bell-LaPadula Model*,* The Biba Model

- The Bell-LaPadula Model **SOS** -> enforce confidentiality by US govt, three rules to enforce confidentiality: 1) Simple SP "no read up" -> a subject cannot read data from a security level higher than subject's security level 2) * SP "no write down" -> a subject cannot write data to a security level lower than the subject's security level 3) Strong * P "no read/write up or down" -> a subject with read/write privilege can perform read/write functions only at the subject's security levels
- The Biba Model **SOS ->** the opposite of Bell-LaPadula, enforce integrity (protection) of knowledge, three rules 1) Simple integrity axiom "no read down" -> a subject cannot read data from an object of lower integrity level 2) * integrity axiom "no write up" -> a subject cannot write data to an object at a higher integrity level 3) invocation property -> a subject cannot invoke (call upon) subjects at a higher integrity level
-

Lesson 3.9: Security Models Part 2

Skills Learned From This Lesson: Security Models*,* Clark-Wilson Model*, Separation of Duties*

- The Clark-Wilson Model -> integrity model, keep users out of your stuff or they will break it, so the user does not access the data directly but through an interface, untrusted never access trusted directly, SEPARATION OF DUTIES, the purpose of an API is exactly this
- This model enforces well-formed transactions through the use of the access triple: User -> Transformation Procedure -> CDI (Constrained Data Item)
-

Lesson 3.10: Security Models Part 3

Skills Learned From This Lesson: Security Models*,* Brewer & Nash Model

- The Brewer & Nash Model a.k.a Chinese Wall -> combat conflict of interest in databases housing competitor information, fair competition, defines a wall and a set of rules to ensure that no subject accesses objects on the other side of the wall, separating competitors data within the same integrated database
-

Lesson 3.11: Security Models Part 4

Skills Learned From This Lesson: Security Models, Security Architecture, Protection Rings

- The Information Flow Model -> Data is compartmentalized based on classification and the need to know, model seeks to eliminate covert channels, data flows from low to high security level and high to low integrity level
- The Non-Interference Model -> actions at a higher security level does not interfere with actions at a lower level, goal is to protect the state of an entity so that data does not pass through covert channels
- The Lattice Model -> the idea of lower and higher boundaries, confidentiality, access to an object by an authorized subject
- Security Architecture -> directs how the components included in the system architecture should be organized to ensure that security requirements are met. It should include: description of locations, description of components, security specifications
- Program -> an application
- Process -> program loaded in memory
- Thread -> individual instruction within a process
- multiprogramming: no true isolation
- Multiprocessing: more than one CPU
- Multithreading: multiple CPUs in the past, multi-core processors provide this today
- CPU modes and protection rings -> Ring 0 (kernel), 1 (OS), 2 (OS and I/O drivers and OS utilities), 3 (Applications and user activity)
- Today there are only 2 rings, fully trusted or fully untrusted
-

Lesson 3.12: System Architecture

Skills Learned From This Lesson: System Perimeter*, Reference Monitor, Secure Modes of Operation*

- Trusted Computer Base (TCB)
- Security Perimeter
- Reference Monitor -> its the law of the system, the rules

- Security Kernel -> it enforces (invoked) the reference monitor concept, it must facilitate isolation of processes, must be invoked at every access attempt, small enough to be tested and verified in a comprehensive manner
- Security Policy -> a set of rules on how resources are managed within a computer system
- Least Privilege -> one process has no more privileges than it needs
- Secure Modes of Operation -> Single State (one classification of data), Multi State (multiple classifications of data), Compartmented (need to know), Dedicated (need to know for everything because there are no compartments)
-

Lesson 3.13: Evaluation Criteria Part 1
Skills Learned From This Lesson: Security Evaluation*, TCSEC, ITSEC*

- Why evaluate? To examine the security-related components of a system, Trust vs. Assurance
- Trust is all about the function of the product eg.auditing, firewall
- Assurance is all about the reliability of the process, was it designed well
- CMMI five maturity levels (Initial, Managed, Defined, Quantitatively Managed, Optimizing)
- The Orange Book (TCSEC) looks trust and assurance as a whole, like a checklist, A1, B1, B2, B3, C1, C2, D
- The Orange Book & the Rainbow Series
- ITSEC (Information Technology Security Evaluation Criteria) created by European Nations in 1991 as a standard to evaluate security attributes of computer systems
- F1 to F10 rates for functionality, E0 to E6 for assurance

Lesson 3.14: Evaluation Criteria Part 2
Skills Learned From This Lesson: Evaluation Criteria*,* Common Criteria, Certification & Accreditation

- Common Criteria ISO 15408
- Protection Profile: requirements from Agency or Customer
- Target of Evaluation (ToE): System Designed by Vendor
- Security target Documentation describing how ToE meets Protection Profile
- Evaluation Assurance Level (EAL 1-7) Describes the level to which ToE
- EAL 4 in the middle - Methodically designed, tested and reviewed

- Certification & Accreditation
- Certification -> technical evaluation of the product, performed by vendor
- Accreditation -> management's approval of the product

Module 4: Communications and Network Security

Lesson 4.1: Introduction to Communications and Network Security
Skills Learned From This Lesson: OSI model, Interoperability, Standardization

- OSI model -> promotes interoperability between vendors, enables standardization, describes the encapsulation (packaging) of data to enable it to get from point A to point B

Lesson 4.2: The OSI Model Part 1
Skills Learned From This Lesson: OSI Model, PDU, SPFB

- You have to know what happens in each layer for the exam
- Protocol Data Unit (PDU) is data in whatever packaging it is. 5,6,7 is data, 4 segments, 3 is a packet, 2 is frame, 1 is bits (D-SPFB)
-

Lesson 4.3: The OSI Model Part 2
Skills Learned From This Lesson: OSI Model, Physical Layer, DataLink Layer

- L1 Physical: physical connectivity, electric signals
- Across layers questions in the exam
- Threats: theft, unauthorized access, vandalism, sniffing, interference, data emanation
- L2 Data Link: LLC - error detection, MAC - Physical
- MAC spoofing
-

Lesson 4.4: The OSI Model Part 3
Skills Learned From This Lesson: MAC Addresses*, ARP, ARP poisoning*

- MAC Addresses
- Address Resolution Protocol (ARP) takes a known IP address and learns and unknown MAC address
- MAC address is cached, the good is don't need to go out and ask again, the bad is that I have old information that I trust

- ARP-Cache poisoning or pollution is the change of cache for the purpose of redirection
-

Lesson 4.5: The OSI Model Part 4

Skills Learned From This Lesson: CSMA/CD*,* CSMA/CA*, Token Passing*

- Carrier Sense Multiple Access with Collision Detection CSMA/CD - Cable-free collision free access, Ethernet 802.3 is collision based and its how the network card determines when to transmit information and when to wait
- Carrier Sense Multiple Access with Collision Avoidance CSMA/CA - 802.11 Wireless
- Token Passing
-

Lesson 4.6: The OSI Model Part 5

Skills Learned From This Lesson: NICs, Sniffers, Switches, RARP

- NICs examine th frame
- Sniffers work in promiscuous mode, which means that they pick up all the data regardless of their MAC address
- Switch -> by default at L2, but more right is both L2 and L3, uses MAC address to direct traffic, isolate traffic into collision domains, does NOT isolate broadcast natively
- Reverse ARP RARP -> predecessor of DHCP, when a client doesn't have an IP, BOOTP NICs operate at L2
- ARP poisoning happen through unsolicited reply
-

Lesson 4.7: The OSI Model Network Devices

Skills Learned From This Lesson: Hub, Switch, collisions

- Hub doesn't do any traffic control, collisions happen, if you plug a sniffer into a hub you will get all the data that passes through the hub
- Each port on a switch is its own collision domain and we want to reduce collision, the switch is our tool
- If I plug a sniffer to a switch port, no traffic should be coming out of the port
-

Lesson 4.8: The OSI Model Collision Domains

Skills Learned From This Lesson: Routers, VLANs, L3 Switches

- Router isolates traffic into broadcast domains and uses IP addressing to direct traffic
- In port by port basis routers are very expensive
- Each port in a router is a subdomain

- VLANs -> to get broadcast isolation on a switch, a VLAN is necessary
- A L2 switch doesn't truly understand L3 IP addressing
- A L3 switch is necessary for inter-Vlan Communication, VLANs cannot talk to each other
- **Routers** are still essential to get off the network, but for internal traffic, **L3 switches** can replace routers and create VLANs
-

Lesson 4.9: The OSI Model Layer 3 Protocols

Skills Learned From This Lesson: L3 Protocols, ICMP, ICMP attacks

- All protocols start with the letter "I" (IP, ICMP, IGMP, IGRP, IPSEC, IKE, ISAKMP) except IMAP
- ICMP -> full of security holes, Ping of Death (big ping packet, MTU size), Ping Flood (many pings), Smurf (spoofed source address and direct broadcasts to launch a DDOS), LOKI attack (hides data inside ICMP messages), fraggle attack (similar to smurf but uses UDP, L4 attack)
- Never allow a directed broadcast, block ICMP at the firewall from outside
-

Lesson 4.10: The OSI Model Layer 4

Skills Learned From This Lesson: UDP, UDP attacks, DNS

- UDP -> connectionless, unreliable, no handshaking, desirable when real time transfer is essential (Media Streaming, Gaming, live chat), FTP uses TCP, TFTP, uses UDP
- SYN flood -> L4 attack
- DNS happens between L5 and L7
-

Lesson 4.11: The OSI Model Layer 5 and 6

Skills Learned From This Lesson: Layer 5 , Layer 6

- L5 -> responsible for establishing a connection between two applications, dialogue control, release connection
- Setup, maintenance and teardown of a communication
- L6 -> present the data in a format that all computers can understand, the only layer that does NOT have any protocols
- Concerned with encryption, compression and formatting
-

Lesson 4.12: The OSI Model Layer 7

Skills Learned From This Lesson: Layer 7, Layer 7 protocols, OSI vs TCP/IP

- L7 -> defines a protocol that two different programs or applications understand
- HTTP, HTTPS, FTP, TFTP, SMTP, SNMP etc.
- Application Proxies
- Non-repudiation
- Certificates, digital signing
- Integration with Directory Services
- Time awareness
- OSI vs. TCP/IP model
-

Lesson 4.13: The OSI Model Firewalls Part 1

Skills Learned From This Lesson: OSI/TCP, Firewalls, HW vs SW Firewalls

- OSI/TCP what you need to know (matrix)
- Firewalls -> isolation and separation, create zones based on trust, HW firewalls vs. SW firewalls, used rule-based access control, whitelisting
- Its not a good idea to take a windows box and make it a firewall (software), because it performs many operations, take an HW firewall that only performs the firewalling tasks, but its more expensive -> cost-benefit analysis
-

Lesson 4.14: The OSI Model Firewalls Part 2

Skills Learned From This Lesson: Firewalls, Layer 3 FW, Defense in Depth

- L3, L5, L7 firewalls
- L3 FW -> packet filtering, screening routers, inspect L3 & L4 Headers (Source and Dest IP, Source and Dest Port, Protocol TCP or UDP)
- The firewall is the first line of defense
-

Lesson 4.15: The OSI Model Firewalls Part 3

Skills Learned From This Lesson: Firewalling, Stateful filtering*, Proxy firewalls*

- As you go up the OSI you get smarter but slower
- L5 Stateful filtering (awareness of the initiation of the session and the state, can block unsolicited replies, can understand the syntax of lower-layer protocols and can block "misbehaving" traffic)
- L7 Application Proxies/firewalls, DPI, forward proxy inspects traffic from inside going out, reverse proxy inspects traffic from outside going in, can inspect on content, time, application-awareness, certificates, specific to the application protocols

- enforce network policy
- rut on the perimeter of a network and allow or deny traffic
- MUST have IP forwarding turned off
- generally, are dual/multi homed
- types of fw (packet filtering, state full, proxy, dynamic packet filtering)
- Packet filter → keeps no state (each packet is evaluated own it's own without regard to previous traffic), Rule-based access control, packet filters are still used on the edge of the network before a stateful fw for performance reasons
- State full fw → router keeps track of a connection in a table. It knows which conversations are active, more complex, and cause DoS against by trying to fill up all the entries in the state tables/use up memory, content dependent access control
- Proxy fw → two types (circuit level, application), both types of Proxies hide the internal hosts/addressing from the outside world
- application proxies → more expensive, advanced logging/auditing and access control features (restrict users to only allowed websites, inspect data for protocol violations, inspect data for malware) extra processing requires extra CPU, proxies only understand the protocols they were written to understand. So you need a separate application proxy for EACH protocol you want to proxy
-

Lesson 4.16: The OSI Model NAT/PAT

Skills Learned From This Lesson: NAT, PAT, fw best practices

- Advantages → you don't need to get real public IP addresses for each computer, RFC 1918 IP addresses, hides internal network structure, transparent
- Disadvantages → Single point of failure/performance bottleneck doesn't protect from bad content
- **overall fw best practices** (block unnecessary ICMP packets, keep ACLS simple, use implicit deny, disallow source-routed packets, use least privilege, block directed IP broadcasts, perform ingress and egress filtering, enable logging, drop fragments or re-assemble fragments
-

Lesson 4.17: Password Security

Skills Learned From This Lesson: Password Security*, password length, password complexity*

- we want security, not always complexity, so a good password could be four random words and not with symbols
-

Lesson 4.18: Area Networks: LAN, WAN and MAN

Skills Learned From This Lesson: WAN network types, circuit switching, packet switching

- two types of WAN networks -> circuit and packet switching
- circuit switching (PSTN, ISDN, DSL, T-carriers)
- packet switching (X.25, Frame Relay, ATM, VOIP, MPLS)
- MPLS creates cost-effective private WANs faster and more secure than regular routed "public" IP networks like the internet, more secure than the public internet because a "virtual" private network end-to-end circuit can be built just for your organization, we don't have to configure and maintain traditional encryption based VPN equipment anymore, provides QoS for VOIP, and other high priority traffic, purely L3 technology
- VOIP → voice over IP, Real-Time Transfer RTP is plaintext, SIP which is used for session initiation, UDP
- Security issues →
    - eavesdropping (greatest threat) – enable S/RTP (Secure/ RTP)
- toll fraud -> used for international calls
- vishing -> social engineering through VOIP
- SPIT -> Spam over IP Telephony
- Performance issues -> latency which is a predictable delay and jittering is an unpredictable delay
-

Lesson 4.19: Remote Access

Skills Learned From This Lesson: Dial up, Tunnelling, authenticity issues

- Dial-Up
    - PPP (L2 framing for remote access, WAN connectivity)
- authenticity through PAP, CHAP, EAP PAP Port Authentication Prot → not good, plaintext, CHAP Challenge Handshake Auth Prot, good because it never puts the password on the network, Zero Knowledge Proof, EAP extensible Auth Prot many different flavors
    - Tunneling
- PPTP only through IP network
- PAP, CHAP, EAP

- MPPE Microsoft Point to Point Encryption
- GRE Generic Route Encapsulation
- L2TP Tunneling protocol no security built-in
- IPSEC
- IPSEC the latest
    - Wireless
- encryption
- WEP, WPA
- WPA II
    - Authentication
- 802.1x
-

Lesson 4.20: General Routing Encapsulation (GRE)

Skills Learned From This Lesson: GRE, GRE attributes, data encapsulation

- point to point link between 2 networks. It adds an extra IP header to the original packet. Much more frequently used in the past to encapsulate AppleTalk, IPX and other older protocols
- Data Encapsulation
- Simplicity
- Multicast traffic forwarding
-

Lesson 4.21: Wireless Security Part 1

Skills Learned From This Lesson: security problems*, WEP, WEP vulnerabilities*

- security problems
    - unauthorized access
    - sniffing unencrypted text
    - Wardriving
    - unauthorized access points (MiTM)

- WEP
    - Shared auth passwords
    - Weak IV (24 bits)
    - IV transmitted in clear text
    - RC-4 stream cipher

- easily crackable
- only adoption for 802.11b

Lesson 4.22: Wireless Security Part 2

Skills Learned From This Lesson: WPA, WPA2, Authentication

WPA

- stronger IV
- Introduced TKIP (Temporal Key Integrity Protocol)- Dynamically negotiated keys as opposed to static in WEP
- Still used RC-4
- Backward compatible with WEP

WPA2

- AES block cipher
- CCMP Counter Mode Cipher Block Chaining Message Authentication Code Protocol -> provides additional encryption strength
- NOT backward compatible

- Authentication
  - WPA and WPA2 Enterprise Uses 802.1X authentication to have individual passwords for individual users (RADIUS)

Lesson 4.23: Wireless Security Part 3

Skills Learned From This Lesson: Bluetooth, Bluetooth modes, Bluetooth attacks

- Bluetooth is a Personal Area Network protocol designed to free devices from physical wires
- Bluetooth modes
  - Discovery Mode
  - Automatic Pairing
  - Blue jacking -> sending SPAM to nearby bluetooth devices
  - Blue Snarfing -> copies information off of remote devices

    - Blue bugging -> more serious, allows full use of phone, allows one to make calls, can eavesdrop on calls
-

Module 5: Identity and Access Management

Lesson 5.1: Introduction to Identity and Access Management Part 1
Skills Learned From This Lesson: IAM, Identification, Authentication

- Identification
    - Identity Proofing
    - Account Provisioning/Deprovisioning

- Authentication
    - Kerberos
    - RADIUS
    - IAM in the Cloud

- Authorization
    - Access Control Models: DAC, MAC, RBAC, RuBAC, ABAC
- Auditing/Accountability

- Identity and Management is the set of processes, procedures, tools, and technology necessary to oversee and manage digital identities
- The goal of IAM is to provide secure and auditable access to the digital resources within an organization
- Revolves around the effective management of the IAAA (Identification, Authentication, Authorization, Auditing/Accounting)
- What can we allow for the ease of use VS. how do we protect it
- Online identity VS. username and password
-

Lesson 5.2: Introduction to Identity and Access Management Part 2
Skills Learned From This Lesson: Identity management, Access Management, *IAAA*

- Identity Management

    - Controls the life cycle for all accounts in a system

- Access Management
    - Controls the assignment of rights/privileges to those accounts
    - Controlling a subjects manipulation of an object

- Per ISC2, Identity and Access Management solutions “focus on harmonizing the provisioning of users and managing their access across multiple systems with different native access control systems”

- IAAA
- Authentication - Type I (Knowledge, something i know), Type II (Possession, something i have), Type III (Biometrics, something I am)
- Single Sign On
- Access Control Models
- Access Control Methods
- Access Control Administration
- Data Emanation

- Access is the data flow between a subject and an object
    - Subject is active- person, process or program
    - Object is passive- a resource, file, printer
    - Access controls should support the CIA triad and regulate what a subjext can do with an object

- Access controls are security mechanisms that control how subjects can interact with objects -> Logical, Physical, Administrative
- Controls should be layered and provide both proactive and reactive protection

- Components of Access Control
    - Identification -> make a claim (userid etc), must be unique for accountability, the identifier should not indicate extra information about user (like job position), can be spoofed

    - Authentication -> Provide support (proof) for your claim, Type I, II, III, can be impersonated -> MFA for stronger auth
-

Lesson 5.3.: Authentication Types Part 1: Something you know
Skills Learned From This Lesson: Type 1, Type 2, Authentication types

- Type 1:
    - Passwords, Passphrases, Cognitive Password
    - Best Practices
        - No less than 8 chars
        - Change on a regular basis
        - Enforce password history
        - Consider brute force and dictionary attacks
        - Ease of cracking cognitive passwords
        - Graphic image
        - Enable clipping levels and respond accordingly

- Type 2:
    - Token Devices
    - Smart card
    - Memory card
    - Hardware key
    - Cryptographic key
    - Certificate
    - Cookies

Lesson 5.4: Authentication Types Part 2: Token Devices
Skills Learned From This Lesson: token devices, Synchronous token devices, Asynchronous token devices

- Token Devices: One time password generators
    - One time password reduces vulnerability associated with sniffing passwords
    - Simple device to implement
    - Can be costly
    - Users can lose or damage

    - Two types: synchronous and asynchronous
-
- Synchronous token devices
- Asynchronous token devices/challenge handshake
    - User logs in
    - Authentication returns a challenge to the user
    - User types challenge string into token device and presses enter
    - Token devices returns a reply
    - Only that specific user's token device could respond with the expected reply
    - More complex than synchronous
    - May provide better protection than sniffing

Lesson 5.5: Authentication Types Part 3: Memory Cards
Skills Learned From This Lesson: Memory cards, Smart cards,

- Memory cards -> hold information, does NOT process
    - A memory card holds authentication info, usually you'll want to pair this with a PIN… WHY?
    - easy to spoof
-
- Smart card
    - More secure than memory cards
    - Can actually process information
    - Includes a microprocessor
    - Often integrated with PKI
    - Two types -> Contact, contactless
-
- Smart card attacks
    - Fault generation
    - Side channel attacks
    - Micro probing
-

Lesson 5.6: Authentication Types Part 4: Something you are
Skills Learned From This Lesson: Biometrics, Biometric Concerns*,*

- Biometrics -> static -> not significantly change over time, fingerprint, hand geometry, iris, retina
    - Dynamic -> very difficult to modify for any significant length of time, voice, gait, signature, keyboard cadence
-
- Biometric Concerns
    - Accuracy
        - Type 1 : False Rejection-> system identifies too much info, excessive overhead
        - Type 2 : False Acceptance->system doesn't evaluate enough information
    - As FRR goes down, FAR goes up and vice versa
    - The level at which the two meet is called CER (Crossover Error Rate), the lower the number, the more accurate the system
    - Iris scan is the most accurate
-

Lesson 5.7: Strong Authentication

Skills Learned From This Lesson: Authorization, Race conditions, Authorization principals

- Strong Auth provides a high level of assurance, always look for more than one type
-
- Authorization -> the concept of ensuring that someone who is authenticated is allowed access to a resource, what rights and permissions you have
- Authorization is a preventative control
- Race conditions would try to cause authorization to happen before authentication, play with time
- Authorization principals -> default NO access (implicit deny), Principle of Least Privilege, need to know, content based
- Authorization creep -> as a subject stays in an environment over time, their permissions accumulate even after they are no longer needed -> auditing authorization can help mitigate this
- Auditing -> logging and reviewing accesses to objects, matching actions to subjects
    - Auditing is a detective control
-

Lesson 5.8: Social Media and the Introduction to Kerberos

Skills Learned From This Lesson: Single Sign On, Social Medial

- Single Sign On -> as environments get larger and more complex it becomes harder and harder to manage users accounts securely
    - Multiple users to create/disable
    - Passwords to remember leads to password security issues
    - Reduces user frustration as well as IT frustration
    - Wastes IT budget trying to manage disparate accounts
-

Lesson 5.9: Kerberos Components

Skills Learned From This Lesson: Kerberos Components*, Single Sign On*

- Very Testable in the exam
- A network auth protocol designed from MIT project Athena. Kerberos tries to ensure auth security in an insecure environment
- Used in Win2000+ and some Unix
- Allows for single sign on
- Never transfers passwords
- Uses symmetric encryption to verify identifications
- Avoids replay attacks
- Essential Components:
    - AS Authentication Server
    - TGS Ticket granting Service
    - KDC Key Distribution Center
    - TGT Ticket Granting Ticket
    - Ticket: means of distributing Session Key
    - Principles (users, applications, services)
    - Kerberos Software (integrated into most OSes)
    - Main Goal: user needs to authenticate himself/herself without sending passwords across the network- needs to prove he knows the password without actually sending it through the wire

- The Kerberos Carnival

Lesson 5.10: The Kerberos Carnival Part 1

Skills Learned From This Lesson: Kerberos functionality

- I need one TGT per login, default is 8 hours or log out

- I send my username to AS and I get a TGT (wrist wrap)
- The TGS gives me a ticket to use the print service
- The password is hashed inside the AS and set aside
- The AS generates the TGT and encrypts it with kelly's password
- So when I want to access a service and enter my password, I decrypt my TGT
- The TGT proves I entered the realm in the right way, it lets me request a TGT from TGS
- The Kerberos ticket is 2 copies of the same session key
- The first copy is encrypted with the user's password
- The second is encrypted with the services password eg. print service so I can access the print service
- Why I don't use asymmetric cryptography? Because I can't guarantee that every domain has a public key infrastructure
- Why I can't use the same ticket for different services? Because the session key is encrypted with the services individual password for every service
-
-

Lesson 5.11: The Kerberos Carnival Part 2

Skills Learned From This Lesson: Kerberos functionality

- KDC = TGS + AS
- Primary Domain Controller PDC Emulator -> the KDC resides
- The fact that I am authenticated doesn't mean that I am authorized, ACLs
- I use Symmetric Cryptography despite the fact it is cumbersome because it fits in every environment
-
-

Module 6: Security Assesment and Testing

Lesson 6.1: The 6 Security Assessments and Testing Objectives

*Skills Learned From This Lesson: I*ntroduction to security assessments

- Introduction to security assessments
- Vulnerability assessments
- Penetration testing
- Remediation
- Intrusion detection

- Audit logs
- Common vulnerabilities
-

Lesson 6.2: Vulnerability Assessments and Penetration Testing
Skills Learned From This Lesson: Vulnerability Assessment, Pen testing, Knowledge Degree

- VA -> physical/administrative/logical
    - Identify weaknesses
    - Just collect information, passive
-
- Pen testing -> ethical hacking to validate discovered weaknesses
    - Red teams (Attack) / Blue teams (defend)

- NIST SP 800-42 guideline on Security Testing

- Degree of Knowledge
    - Zero-Knowledge (Black Box Testing): this simulates an external attack
    - Partial Knowledge: limited knowledge of the organization
    - Full Knowledge: this simulates an internal attack

-

Lesson 6.3: Vulnerability Scanning
Skills Learned From This Lesson: Vulnerability Scanning*,* Attack Methodology, rootkit infection

- Vulnerability Scanning
    - Identifying
        - Active hosts on the network
        - Active and vulnerable services (ports) on hosts
        - Applications
        - OSes
        - Vulnerabilities associated with discovered OS & apps
        - Misconfigured settings

    Testing compliance with host application usage/security policies
    Establishing a foundation for pen testing
-
- Attack Methodology

    - Recon (whois, company website, social engineering)
    - Footprinting (nmap, ICMP, DNS zone transfer)
    - Fingerprinting (identify host info, port scanning)
    - VA
    - Attack (pen test, privilege escalation, rootkit, cover tracks)

- Infected from rootkit -> wipe the drive, install OS from original media, restore data from backup
-

Lesson 6.4: Testing Guidelines

Skills Learned From This Lesson: Testing Guidelines, Pen testing considerations

- Why test?
    - Risk analysis
    - Certification
    - Accreditation
    - Security architectures
    - Policy development
-
- Develop a cohesive, well planned, and operational security testing program
-
- Pen testing considerations
    - 3 basic requirements -> meet with senior mgmt to determine the goals, document ROE, get sign off from Senior Mgmt
    - Issue: it could disrupt productivity and systems
    - Tester should determine the effectiveness of safeguards and identify areas of improvement -> TESTER SHOULD NOT BE THE ONE SUGGESTING REMEDIATION. THIS VIOLATES SEPARATION OF DUTIES

Lesson 6.5: Rules of Engagement Part 1

Skills Learned From This Lesson: ROE, Approaches to Testing, Network Scanning

- Specific IP addresses/ranges to be tested (any restricted hosts)
- A list of acceptable testing techniques
- Times when testing is to be conducted

- Points of contact for the pen test team, the targeted systems, and the networks
- Measures to prevent law enforcement being called with false alarms
- Handling of information collected by pen test team

Approaches to Testing

- Do not rely on single method of attack
    - Get creative
- Path of least resistance
    - Start with users - social engineering is often the easiest way
- Break the rules
    - Attempt things not expected
- Do not rely exclusively on high tech tools
- Do not damage systems or data
- Do not overlook small weaknesses in search of the big ones
- Have a toolkit of techniques

Network Scanning

Password Cracking

Rogue infrastructures (unauthorized DHCP servers, DNS servers)

Lesson 6.6: Rules of Engagement Part 2

Skills Learned From This Lesson: War Dialing, Corrective Actions, Watching Network Traffic

- War Dialing
    - Goal is to discover unauthorized modems
    - Dial large blocks of phone numbers in search of available modems
    - Includes all numbers that belong to an organization, except those that could be impacted negatively
    - If removal is not possible, block inbound calls to the modem
-
- War Driving -> looking for unprotected signal

Corrective Actions

- Investigate and disconnect unauthorized hosts
- Disable unnecessary and vulnerable services
- Modify vulnerable hosts to restrict access to vulnerable services
- Modify enterprise firewalls
- Upgrade vulnerable systems
- Deploy mitigating countermeasures
- Monitor vulnerability alerts
- Modify security policies
- **All of the above require going through proper change mgmt procedures**

Side channel Attacks - Traffic Analysis -> I want to know where data is going, i am looking at the actual data
Traffic Padding -> add some unnecessary traffic to make difficult to determine which systems are receiving the legitimate traffic

Lesson 6.7: Protocol Analyzers (Sniffers) and Privacy
Skills Learned From This Lesson: Sniffers, IDS

- Sniffer uses a NIC in Promiscuous mode
- Packet Sniffer + Analysis Engine = Intrusion Detection System
  IDS
- Identify suspicious activity
- Log activity
- Respond (alert people)
- Needs an interface in “promiscuous” mode
- Port mirroring/span needs to be enabled to view traffic on a switch
-
-

Lesson 6.8: IDS Part 1
Skills Learned From This Lesson: HIDS, NIDS, IDS vs. IPS

- HIDS - NIDS

IDS Components

- Sensor - Data Collector -> on network segments (NIDS) or on hosts (HIDS)
- Analysis Engine
- Signature Database
- User Interface and Reporting

HIDS -> examine operation of a single system independently to determine of anything “of note” is going on
HIDS looks at:

Logins
System log files/audit files
File activity/changes to software
Configuration file changes
Processes being launched or stopped
Use of certain programs
CPU usage
Network traffic to/from computer

Pros of HIDS -> can be OS and application specific, they can look at data after its been decrypted (network traffic is often encrypted)

Cons of HIDS -> only protect one machine

Use local system resources
Don't see whats going on, on other machines
Scalability
HIDS could be disabled if machine is hacked

NIDS -> watch en entire network and all associated machines. Looks at SRC IP, DEST IP, Protocol, Port Numbers, Data Content
A NIDS will look for DoS Attacks, Port Scans, Malicious Content, Vulnerability Tests, Tunneling, Brute Force Attacks, Policy Violations eg. Detect Instant Messaging or streaming video

Pros of NIDS -> a single NIDS can cover a whole network

Deployment is usually easier

A NIDS can see things that are happening on multiple machines, it gets a bigger picture and may see distributed attacks that a HIDS would miss

Cons of NIDS -> Data must be unencrypted for a NIDS to analyze.
Switches cause problems for NIDS- port span should be implemented on the switch port
If only on the perimeter, it can miss things on the inside
It must be able to handle LOTS of data to be effective
It does not see what's going on a server directly

IDS vs. IPS

IDS is passive
An IPS is an IDS that takes an active approach eg. Activate FW rules dynamically, shuts down TCP traffic

Lesson 6.9: IDS Part 2
Skills Learned From This Lesson: Analysis Engines, Pattern Matching, Bypassing an IDS

- Analysis Engines
  - Pattern matching (Signature Based) -> does not protect against 0day attacks
  - Profile Matching (Anomaly/Behavior/Heuristics) -> look for changes in normal behavior
    - Advantages -> can possibly detect 0days, can detect behavioral changes that might not be technical attacks
    - Disadvantages -> lots of false positives, often ignored due to the reason above, requires a much more skilled analyst
- Bypassing an IDS
  - Evasion Attack -> many small attacks from different directions, salami attack
  - Insertion attack -> adding meaningless information to a known attack
-

Lesson 6.10: IDS Part 3
Skills Learned From This Lesson: Rule Based, Honeypot, Padded Shell

- Rules Based
  - Uses expert system/knowledge

- These use a database of knowledge and an “inference engine”

Promiscuous Mode -> to accomplish sniffing network analysis, or IDS functionality, you have to put network interfaces into promiscuous mode

Honeypot -> Deployment -> pseudo flaw, sacrificial lamb system on the network
Be careful of Enticement (look appealing) vs. Entrapment (click here to win)

-

Padded Shell and Vuln Tools
Concept used in software programming where a “safe” environment is created for applications and processes to run in -> Similar to a virtual machine

Concept used in IDS where identified intruder is moved to a “safe” environment without their knowing

Simulated environment to keep intruder happy and busy-> hopefully leave production sustems alone

aka. : Self Mutating Honeypot, Tarpit

Module 7: Security Operations

Lesson 7.1: Security Incident Response
Skills Learned From This Lesson: Incident Response, Computer Forensics, Digital Evidence Rules

- Event -> a change in state
- Incident -> Series of events that has a negative impact on the company and its security
- IR focuses on containing the damage of an attack and restoring normal operations
- Investigation focuses on gathering evidence of an attack with the goal of prosecuting the attacker
- Framework should include -> response capability, IR and handling, Recovery and Feedback
- IR -> policies, procedures, guidelines

- Legal, HR, Executive mgmt must be involved
- If handling in-house, an ir team must be in place
  - List of outside agencies and resources to contact (CERT)
  - List of computer or forensics experts to contact
  - Steps on how to secure and preserve evidence
  - Steps on how to search for evidence
  - List of items that should be included on the report
  - List of how different systems should be treated in this type of situation

IR and Handling
Triage
Detection
Identification
Notification
Investigations
Containment
Analysis and Tracking

Recovery and Feedback -> restoration of the system to operations. It must provide greater security or will fall prey to the same attack again
Provide feedback -> very important and often overlooked. Document, document, document.
Computer forensics

Five rules of Digital Evidence -> Digital Evidence must:
Be authentic -> guarantee it hasn't be changed, hashing
Be accurate -> complete, no only portion, convincing
Be complete ->
Be convincing -> furthing appoint
Be admissible ->

Lesson 7.2: The Forensics Investigation Process Part 1
Skills Learned From This Lesson: Forensic Investigation Process*, Identification, Preservation*

- Forensic Investigation Process -> Identification, Preservation, Collection, Examination, Analysis, Presentation, Decision
- Identification -> Locard's principle
- Preservation -> Chain of Custody must be well documented
- Collection -> minimize handling/corruption of evidence
-

Lesson 7.3: The Forensics Investigation Process Part 2
Skills Learned From This Lesson: Forensic Investigation Process*, Examination, Analysis*

- Examination -> look for signatures of known attacks
- Analysis -> primary image vs. working image, root cause
- Presentation -> interpreting the results of the investigation and presenting findings, documentation
- Decision ->Suspects, Corrective Actions
-

Lesson 7.4: Evidence Types
Skills Learned From This Lesson: Evidence Life Cycle*,* Evidence Types*,* Suspect's Actions

- Evidence Life Cycle
- Integrity and authenticity of evidence must be preserved throughout the life cycle
- Evidence Types ->
    - direct evidence (can prove a fact by itself and does not need backup info)
    - real evidence (physical evidence)
    - best evidence (most reliable)
    - Secondary (not strong enough to stand alone, but can support other evidence)
    - Corroborative Evidence (support evidence)
    - Circumstantial (proves one fact which can be used to reasonably to suggest another)
    - Hearsay (2nd hand oral or written)
    - Demonstrative (presentation based)
- Who should do the investigation? Law enforcement
- Suspect's Actions and intent
    - Enticement (tempting a potential criminal, legal and ethical, honeypot)
    - Entrapment (tricking a person into committing a crime, illegal and unethical)
-

Lesson 7.5: Fault Management

Skills Learned From This Lesson: Spares, RAID, Redundant Servers

- Spares (Redundant HW, SLAs, MTBF and MTTR)
- RAID-0 -> Disk striping provides no redundancy or fault tolerance
- RAID-1 -> Disk Mirroring-Provides redundancy but is often considered to be the least efficient usage of space
- RAID-5 -> Disk Striping with Parity: Fault tolerance + speed
- Redundant Servers -> primary server mirrors data to secondary server
- UPS -> size of load UPS can support, how long it can support this load, physical space required, long battery life
- Clustering-> group of servers that are managed as a single system
-

Lesson 7.6: Backups

Skills Learned From This Lesson: Backup types, Backup Issues, Redundancy of Staff

- Shadowing, Remote Journaling, Electronic Vaulting
- Backups -> backing up SW and having backup HW is a large part of network availability
    - Full backup -> archive bit is reset
    - Incremental Backup -> backs up all files that have been modified since last backup
    - Differential backup -> backs up all files that have been modified since last full backup
    - Copy backup -> same as full backup, but archive Bit is not reset
    - Backup issues -> identify what needs to be backed up first
- Redundancy of Staff
    - Eliminate Single Point of Failure
    - Cross Training
    - Job Rotation
    - Mandatory Vacations
    - Training and Education
- Business Continuity
-

Module 8: Software Development Security

Lesson 8.1: Introduction to Software Development Security

Skills Learned From This Lesson: Design Process, Attack Surface, Threat Modeling

- Design Process -> reduce the Attack Surface, Threat Modeling, Risks in Design, Controls Evaluation
- Reducing the attack Surface of the product ->
    - User input fields
    - Protocol/Services/Interfaces/Processes
    - Resource files
    - Open named pipes/open sockets
    - How many items are accessible
    - Dynamic web pages
    - Guest accounts enabled
    - ACL configuration
- Threat Modeling
    - Identify Security Objectives
    - CIA Triad
    - Tools for Threat Modeling
    - STRIDE Mitigation(Spoofing,Tampering, Repudiation, Denial of Service, Escalation of Privilege)

- Controls Evaluation
    - Efficacy of Controls
    - Economy of Mechanism
    - Cost/Benefit Analysis
    - Psychological Acceptability
-

Lesson 8.2: Secure Design

Skills Learned From This Lesson: Secure design, Design Considerations, Risks in Design

- Design Considerations
    - CIA triad
    - Authentication,Authorization,Auditability
    - Secure Design Principles

- Risks in Design
    - Code reuse
    - Flaws (Inherent fault with the design of code) vs. Bugs (implementation fault)

    - Open vs. Closed Design

- Secure Software Development Methodologies
    - Secure Software Development Terms
    - Principles of Secure Design (Least Privilege, Separation of Duties, layered Defense, Fail Secure, Economy of Mechanism, Open, Complete Mediation, Psychological Acceptance, Leveraging Existing Components, Redundancy)
    - Secure Coding Concepts
    - Secure Software Development Lifecycle
    - Common Methodologies
- Security vs. Quality
    - Quality:Fitness for use. Degree to which a product meets its requirements. Does it do what it is supposed to do?
    - Security: reducing probability or impact of vulnerabilities
-

Lesson 8.3: Requirements to Writing Secure Code
Skills Learned From This Lesson: Secure Code*, Bug Tracking, DREAD*

- Training and Awareness for Developers
- Shift of focus/understanding for managers
- Security Checkpoints and Reviews
- Bug tracking
    - Classification of bugs uses DREAD
    - D -> Damage potential
    - R -> Reproducibility
    - E -> Exploitability
    - A -> Affected user base
    - D -> Discoverability
-

Lesson 8.4: Software Development Methodologies
Skills Learned From This Lesson: Software Development*, Waterfall, Prototyping*

- Waterfall : unidirectional Sequential phased approach
- Prototype
- Spiral
- Agile

-

Lesson 8.5: Cloud Application Security
Skills Learned From This Lesson: Cloud Security

- Determine Data Sensitivity
- Cloud Application Architecture
- Security Responsibilities Across Models
- The Software Development Lifecycle
- OWASP Top Ten Vulns
- IAM and Federated identity management
- Application Security Testing
-

Lesson 8.6: OWASP (Open Web Application Security Project)
Skills Learned From This Lesson: OWASP top ten

- Designed to raise awareness and to stress the need for security in web-based applications
- 1)Injection
- 2)Broken Authentication
- 3)Sensitive Data Exposure
- 4)XML External Entities (XXE)
- 5)Broken Access Control
- 6)Security Misconfiguration
- 7)Cross-Site Scripting (XSS)
- 8)Insecure Deserialization
- 9)Using Components with Known Vulnerabilities
- 10)Insufficient Logging & Monitoring
-

Lesson 8.7: Organizational Normative Framework
Skills Learned From This Lesson: Organizational Normative Framework*, Validation, Verificationl*

- Specified in ISO 27034
- Defines Components of application security best practices
    - Business Context
    - Regulatory Context
    - Technical Context
    - Specifications

    - Roles
    - Processes
    - ASC Library
- Application Normative Framework -> Used in conjunction with the ONF and is created for specific applications, think of best practices for applications within the context of the organization
- Common SW vulns and countermeasures agenda
    - Why is software unsecure? Lack of training, funding, no prioritization of security, security as an afterthought
    - Vuln databases and resources
    - Types of vulns
        - Overflows
        - Injections
        - XSS
        - CSRF
        - Misconfigurations
        - Disclosure
        - Race Conditions
        - Side Channel Attacks
        - File Attacks
- Validation -> it serves the purpose it needed to serve, management acceptance, is this what you wanted?
- Verification -> correctness of the product, usually internal, assessment, technical testing
- Certification -> the product meets its requirements, technical verification
- Post acceptance -> ongoing updates, patches, and changes reviewed and applied

Lesson 8.8: Object-Oriented Programming
Skills Learned From This Lesson: OOP, Classes, Objects

- Most widely used approach to SW development
- Traditional programming input->Processing->output
- OOP is modular in nature and focuses on the solution of problems through objects, classes, methods, functions
- A Class is a concept
- An Object brings that concept to life

-

Lesson 8.9: Database Introduction Part 1

Skills Learned From This Lesson: DB models, Hierarchical, Distributed

- DB Models
    - Describes relationships between data elements
    - Used to represent the conceptual organization of data
    - Formal methods of representing information
    - Hierarchical-> tree like fashion, info from major group to subgroup
    - Distributed -> client server type of DB located on more than one server distributed in several locations
    - Object-Oriented
    - Relational
-

Lesson 8.10: Database Introduction Part 2

Skills Learned From This Lesson: Relational DB, Primary key *, Normalization*

- Primary key -> uniquely identifies each record as unique
- Entity Integrity -> Primary key cannot be null
- Normalization -> each attribute in a database must describe ONLY the primary key. Provides a means for removing duplicates
- Fields, Columns, Attributes -> mean the same
- Record, Rows, Tuples -> mean the same
-

Lesson 8.11: Database Introduction Part 3

Skills Learned From This Lesson: Attributes, Tuples, Foreign key

- Attributes -> Individual descriptors
- Tuples is data in rows
- Foreign key is when a PK from one table appears in a secondary table
-

Lesson 8.12: Database Introduction Part 4

Skills Learned From This Lesson: Cardinality, Schema, DB Schema

- Cardinality -> number of rows in a relation
- Degree -> number of columns in a relation
- DB Schema -> defines the design, structure
-

Lesson 8.13: Database Introduction Part 5
Skills Learned From This Lesson: DB Vulns, Inference, Polyinstantiation

- DB Vulns, threats and Protections
    - Aggregation
    - Inference
    - Polyinstantiation -> multiple instances, lots of unclassified info can lead to classified clue
    - Code Injection
    - Input Validation

Lesson 8.14: Database Introduction Part 6
Skills Learned From This Lesson: ACID test, ACID, Malware

- *Doed the DB pass the ACID test?*
- ACID
    - Atomicity -> transactions are either fully committed or rolled back
    - Consistency -> DB rules are enforced
    - Isolation -> transactions are invisible until committed
    - Durability -> once commit has been received, the transaction cannot be rolled back
- Beyond the traditional DB
    -

- Data-> information -> Knowledge
- Malware types