*These notes were made following the* ***TOTAL: CompTIA Security+ Certification (SY0-501) course from Mike Meyers and Total Seminars.***

* + **Section 1: Risk Management**
    - CIA of Security
      * CIA Triad (Goals of Security)
        + Confidentiality
        + Integrity
        + Availability
      * Confidentiality: Keeping data secret from anyone who shouldn't be accessing it.
      * Integrity: Ensures data and systems is in an unaltered state when stored, transmitted, or received.
      * Availability: Ensures systems and data is available to authorized users when needed.
      * Also added:
        + Auditing & Accountability: Keeping track of what goes on (logs).
        + Non-Repudiation: Ties into accountability; making it to where users cannot deny an action.
    - Risk Management
      * Identification, assessment, and prioritization of risk.
      * Potential to harm organizations, people, systems.
        + Assets

Any part of our infrastructure that we protect.

Servers, routers, firewalls, systems.

People.

Server room doors, physical aspects.

* + - * + Vulnerabilities

A weakness to an asset to be exploited.

Default passwords on equipment.

Server room that is unlocked.

* + - * + Threats

A negative event or action that exploits a vulnerability.

An actual login attempt by hacker.

* + - * + Threat agent

A person or entity that follows throw with the threat.

* + - * + Likelihood

A level of certainty that a negative event will happen.

Often an annualized basis or percentage.

Two ways to measure likelihood:

Quantitative: A power supply for a Cisco device dying. (10%.)

Qualitative: Customer loyalty after a bad event. (Low, medium, high.)

* + - * + Impact

Harm caused by a threat.

Preceded by a negative event happened.

Quantitative values: Cost, labor, time.

Qualitative values: Reputation, name recognition.

* + - * Threats -> vulnerabilities = risk
      * NIST SP 800-30 is a standard document of risks and vulnerabilities and is an industry standard.
    - Threat actors
      * Attributes:
        + Internal/external: Are these threat actors within the company or in a different country?
        + Level of sophistication: Threat actors can wreak havoc on basic levels or be very sophisticated and experiences.
        + Resources and funding: How much funding and willingness exists for threat actors to carry out their tasks?
        + Intent: What is the intention? Money? White hat, black hat.
        + Open-Source Intelligence (OSINT): Social media, public records.
      * Types of threat actors:
        + Script kiddies (skiddies)

Trivial attack knowledge

Use scripts and pre-made tools

Most cases are easily preventable.

* + - * + Hacktivist

Intent is motivation of activism

* + - * + Organized Crime

Smart groups of hackers to make money

* + - * + Nation states/Advanced Persistent Threat (APT)

Motivation is intelligence and sensitive information

Sophisticated toolsets.

APTs gain access to a system and stay put, continuing to funnel information.

* + - * + Insiders

Not always an employee - could be anyone within the infrastructure/organization.

Do they have access to information? (Usernames/passwords)

* + - * + Competitors

Not as big of an issue in today's society due to private business laws.

* + - * Keep in mind, what are the attributes to be applied to each threat actor?
    - Managing Risk
      * Risk Identification/Assessment
        + Catalog and define all assets/Vulnerability Assessment

What are the vulnerabilities of our assets?

NIST SP 800-37 summarizes vulnerabilities of assets, but very broad.

cve.mitre.org

Common Vulnerabilities and Exposure Database

Administered by the Mitre Corporation

Goes into detail about vulnerabilities

Example: Mail application built-into Osx 8.0 or earlier vulnerable to sniffing.

Nessus, which is a program ran on the LAN that generates a report of vulnerabilities, is used quite often.

Penetration (pen) testing

Outside party of some sort looks for vulnerabilities and ways to exploit them, and reporting to the company.

* + - * + Threat Assessment

Looking to define threats applicable to our infrastructure.

Adversarial threats:

Hacker, malware, etc.

Accidental threats:

User accidentally corrupts database.

Administrator accidentally reformats HDD on a server.

People who have permissions to cause damage, but done on accident.

Structural:

Power supply dies, camera goes out, equipment failure, software failure.

Environmental:

Fires, water, AC going out causing overheating.

* + - * + Risk Response

Opportunities:

Mitigation: Applying a security control to a particular risk.

Risk Transference: Offloading some likelihood, risk, and impact onto a third party. (Example: moving a server to the cloud.)

Risk Acceptance: Where the likelihood and impact of a risk is less than the cost of mitigating the risk.

Risk Avoidance: This particular combination of risk and likelihood is too high to even consider, so dropping the risk all together.

* + - * + Frameworks

A workflow or methodology, or an idea of a process to deal with risk management.

Sources of two commonly used frameworks:

NIST Risk Management Framework Special Publication 800-37

ISACA Risk IT Framework

Boils down to: assessment, applying security controls, monitor the situation, respond to any risks; then the process continues in a circular motion.

* + - Using guides for Risk Assessment
      * CompTIA views this as "How do we secure stuff?" in a broad stroke.
      * Types of guides:
        + Benchmark: A company who sells a router should tell you what percentage of CPU usage at any time.

We can do our own benchmarks, such as running a benchmarking tool on a machine to check network throughput, etc.

Use threshold values to verify expected throughput or action.

* + - * + Secure Configuration Guides:

Routes, operating systems, wireless access points - all of these devices have a "proper" or "recommended" configuration.

Platform and vendor guides.

Examples:

Apache Security Tips for their web server.

Windows guide for "Configure Web Server Security (IIS 7).

NIST provides guides for securing operating systems, such as "Guide to Securing Apple OS X 10.10 Systems for IT Professionals"

Network Infrastructure Devices:

Examples:

Beginner's Guide to EdgeRouter (for Ubiquiti)

NIST Guide SP 800-153 "Guidelines for Securing WLANs"

General Purpose Guides:

Lists of security controls, in a general sense, to apply.

Example:

NIST SP 800-123 "Guide to General Server Security"

Broad, less specific topics, such as: user accounts, password policies, intrusion protection, etc.

* + - Security Controls
      * A verb or action, a mechanism applied to our IT infrastructure to protect from security problems or remediate existing security problems.
      * Not just IT security - physical building security, phishing training for employees, etc.
      * Apply, monitor, and applying security controls to IT infrastructure.
      * Broken into categories:
        + Administrative Control (Management Control)

Controls actions people make towards IT security.

Laws

Policies

Guidelines

Best practices

What do people do?

* + - * + Technical Control

Controls actions IT systems make towards IT security.

Computer stuff

Firewalls

Password links

Authentication

Encryption

* + - * + Physical Control

Controls actions in the real world.

Gates

Guards

Keys

Man traps

* + - * Security Control Functions:
        + Deterrent

Deters the actor from attempting the threat

* + - * + Preventative

Deters the actor from performing the threat

* + - * + Detective

Recognizes an actor's threat, may or may not do anything about it.

* + - * + Corrective

Mitigates the impact of a manifested threat

* + - * + Compensating

Provides alternative or temporary fixes to any of the above functions.

* + - Interesting Security Controls
      * Mandatory Vacation
        + Requires individuals to take vacation - used to detect fraud and unauthorized activity.
      * Job Rotation
        + Periodically switching people around to different positions, also avoids contempt of position.
      * Multi-Person Control
        + More than one person is needed to accomplish a task or function, and also allows multiple people to make sure it is done correctly.
      * Separation of Duties
        + Administrative control. Single individuals should not perform all critical or privileged duties across the board.
      * Principle of Least Privilege
        + Users granted only the level of privilege that is needed for their job.

* + Defense in Depth
    - AKA, Layered Security.
    - Diversity vs. Redundancy
      * Redundancy is the same type of security control implemented over and over again.
      * Diversity is varying controls implemented at once.
    - Defense in depth is typically discussed in regards to a variety of physical, administrative, and technical controls.
    - Vendor diversity is a method of defense in depth with technical controls.
  + Security Governance
    - Governance is a set of overarching rules that defines how an organization and its personnel conduct themselves.
    - IT Security Governance is a set of overarching rules that defines how an organization and its personnel conduct IT security.
    - Sources of Security Controls:
    - Laws and Regulations
      * Example: HIPAA
    - Standards
      * Government Standards: NIST or ISO
      * Industry Standards: PCI-DSS (Credit card standards)
    - Best Practices
      * Microsoft Best Practices
    - Common Sense & Experience
      * What has worked in the past? What do I think is the best way to do something?
    - Creating policies:
      * Broad in nature
      * Used as directives
      * Define roles and responsibilities
    - Organization standards define the acceptable level of performance of policy.
    - Security controls come from the policies and standards.
    - A procedure is a step-by-step process of how we do a task.
    - Securitu Controls 
      Laws and Regulations Common Sense 
      Best Practices 
      Policies 
      Standards 
    - Guidelines
      * A guideline is considered optional.
      * Not clearly defined.
      * Just an idea of how we should tend to do something.
  + Security Policies
    - Acceptable Use Policy
      * Most well-known.
      * Defines what a person can or can not do when using company assets.
      * Uses very broad strokes.
    - Data Sensitivity and Classification Policies
      * Defines importance or nature of data.
      * Applying labels to types of data (top secret, secret, confidential, etc.)
    - Access Control Policies
      * Defines how someone gets access to data or resources.
      * Can cover passwords, fobs, smart cards, etc. Defines what type of data users have access to.
      * Addresses data access and classification restrictions.
      * Can be incorporated into Acceptable Use Policy, Data Classification Policy, etc.
    - Password Policy
      * Defines how we deal with passwords.
      * Typically incorporated into other documents.
      * Covers password recovery/loss.
      * Bad login attempts.
      * Password retention and reuse policies.
    - Care and Use of Equipment
      * Often under Acceptable Use Policy.
      * Covers maintenance of equipment, how to borrow/check out equipment, responsibility matrixes.
    - Privacy Policies
      * Applied to customers and in-house.
      * Common among social media for customers of that media.
    - Personnel Policies
      * Deals with the people dealing with our data.
      * Background checks, security clearances, etc.
      * "We will use job rotation and mandatory vacations."
      * If it has to do with a person, and a person dealing with data, it goes in a personnel policies.
  + Frameworks
    - Nothing more than a process idea. Provides organization for good IT security infrastructure.
    - Types of Frameworks:
      * Regulatory
      * Non-Regulatory
      * National standards
      * International standards
      * Industry-specific frameworks
    - Examples of Frameworks:
      * NIST SP800-37 - National standard and US federal regulatory.
      * ISACA IT Infrastructure - Non-regulatory.
      * ISO 27000 - International standard
    - NIST Risk Management Framework
      * Risk Management Framework 
        CATEGORIZE 
        MONITOR 
        AUTHORIZE 
        ASSESS 
        SELECT 
        IMPLEMENT 
      * Categorize workflows, processes, vendors, organizational inputs/outputs.
      * Select security controls - look at what is taking place, and based on regulations/laws/best practices, etc. - choose what to implement.
      * Implement security controls.
      * Assess security controls once implemented. Verify that everything works the way it is supposed to. Often done in a sandbox.
      * Authorize information systems. Creates lessons learned, and establishes hierarchy of responsibility.
      * Monitor security controls. Watch the controls and making sure it is mitigating/eliminating risk, not impacting users' lives too severely, etc.
  + Quantitative Risk Calculations
    - Asset value
      * Not just the cost of an item. For example:
        + A router costs $2500. Factor in cost of a technician to replace it, and how much money/productivity is lost during the downtime. (Router = $2500, plus $500/day for a technician, plus the $2000 lost per day makes the asset value $5000.)
    - Exposure Factor
      * Percentage of an asset that's lost as a result of an incident.
      * A router that, if shorted, would be a full loss; would be an EF of 1.
      * A server room that, if flooded, would only have some items damaged, could be an EF of .75.
    - Asset Value x Exposure Factor = Single Loss Expectancy
      * The $5000 asset value of the router example, at an exposure factor of 1 (5000 x 1 = 5000).
    - Annualized Rate of Occurrence = in a given year, what are the chances of this particular instance taking place.
      * If it floods once every twenty years, that would be .05.
    - SLE x ARO = Annualized Loss Expectancy
    - Good 
      MTTF 
      Foiled 
      MTBF 
      MTTF 
      MTTR 
      Time 
    - MTTF - Mean Time To Failure - Usually applied to an item that cannot be repaired.
    - MTTR - Mean Time To Repair
    - MTBF - Mean Time Between Failures - Usually applied to an item that can be repaired.
  + Business Impact Analysis
    - The study and analysis of the impact on the organization when a disruption occurs.
    - BIA Basics:
      * Determine mission process. What are the things that we do within our IT infrastructure to perform our jobs?
      * Identify critical systems. If our modem is not working, we cannot do our jobs.
      * Single point-of-failure. Set up redundancy to minimize this.
      * Identify resource requirements. In order to access payroll files, we need the servers that store them to be available.
      * Identify recovery priorities. If everything goes down, what are the priorities to make the business recover best?
    - Impact examples:
      * Monetary loss
      * Property loss
      * People
        + Safety
        + Life
      * Finance
        + Ability to create revenue. Cash flow. Credit. Payroll.
      * Reputation
    - Privacy Impact Assessment (PIA)
      * What will the impact be to us if the private data we control were breached?
      * PII (Personally Identifiable Information)
      * PHI (Personal Health Information)
    - Privacy Threshold Assessment (PTA)
      * What is this data? Where is this data? How are we storing this data?
    - A PIA and PTA are both done in order to understand what the impact what the loss of personal information can do to a business.
    - Recovery Time Objective (RTO)
      * The minimum time necessary to restore a critical system operation. The maximum time a critical system can be down without substantial impact.
    - Recovery Point Objective (RPO)
      * Maximum amount data that can be lost without substantial impact.
  + Organizing Data
    - Data Labeling allows recipients of the data to know if or how the data can be shared.
    - Data types:
      * Public data is data that has no restriction, within the public domain.
      * Confidential data is data that one party offers to a second party, but only to that party. Limited to authorized viewing.
      * Private information is information that is limited to only the individual to whom the information is shared. Personally Identifiable Information (PII).
      * Proprietary is private information at a corporate level.
      * Protected Health Information (PHI) is any information pertaining to the health of a particular person. Health Insurance Portability and Accountability Act (HIPAA).
    - Data roles:
      * Owner of the data. Person/entity who has the legal responsibility for the data.
      * Steward/custodian, who is meant to maintain the accuracy and integrity of data.
      * Privacy Officer is the person who is in charge of ensuring data adheres to privacy policies and procedures.
    - Data users:
      * Users. Assigned standard permissions to complete task.
      * Privileged users. Increased access and control relative to a user.
      * Executive users. The user who makes strategic decisions, sets policies on data and incident response actions.
      * System administrators. Has access to delete entire databases, set permissions on all others, etc.
      * Data owner/system owner. People or organizations who have legal ownership of particular dataset or system.
  + Security Training
    - Onboarding is the process that takes an entity outside of your infrastructure that brings that entity into your infrastructure.
      * Requires background check.
      * Non-disclosure agreement (NDA)
      * Standard operating procedures.
      * Specialized issues. (Requirement of clean desk, etc.)
      * Rules of behavior (Good acceptable use policy)
      * General security policies. (Social media use, etc.)
    - Offboarding is the process in which someone leaves your infrastructure.
      * Disable accounts
        + Never delete.
      * Return credentials
      * Exit interview
      * Knowledge transfer
    - PII is a huge part of training for legality's sake, stolen information, etc.
    - NIST 800-122 goes into great detail on the concept of PII.
      * Information to watch out for:
        + Full name
        + Home address
        + Email address
        + National Identification number (social security)
        + Passport number
        + Vehicle registration plate number
        + Driver's license number
        + Face, fingerprints, or handwriting
        + Credit card numbers
        + Digital Identity
        + Date of birth
    - Personnel Management Controls
      * What people do in terms of work to keep our infrastructure as secure as possible.
      * Examples:
        + Mandatory vacations

Verifies dependency issues

Prevents collusion

Makes fraud more difficult

* + - * + Job rotation

Redundancy and backup

Makes fraud more difficult

Allows for cross-training

* + - * + Separation of duties

Requires dual or more execution

* + - Role-based Data Controls
      * System owner
        + Management level
        + Maintains security of the system
        + Defines a system administrator
        + Works with all data owners to ensure data security
      * System administrator
        + Assigned by system owner to perform day-to-day administration
        + Implements security controls
      * Data owner
        + Defines sensitivity of data
        + Defines protection of the data
        + Works with system owner to protect data
        + Defines access to the data
      * User
        + Accesses and uses the assigned data responsibility
        + Monitors and reports security breaches
      * Privileged user
        + Has special access to the data beyond the user
        + Works closely with system administrators to adhere to security
      * Executive user
        + Read only access to all data on system
  + Third party agreements
    - Business Partners Agreement (BPA)
      * Includes primary entities, time frame, financial issues, management.
    - Service Level Agreement (SLA)
      * Includes service to be provided, minimum up-time, response time (contacts), start and end date.
    - Interconnection Security Agreement (ISA)
      * NIST 800-47
      * Statements of requirement (Why are we interconnecting? Who is interconnecting?)
      * System security considerations (What information is interconnecting? Where is this information going? What services are involved? What encryption is needed?)
      * Topological drawings.
      * Signature authority (timeframe, technical reviews, security reviews)
    - Memorandum of Understanding/Agreements (MOU/MOA)
      * ISA's are typically reinforced by these.
      * Not a contract, but looks like one.
      * Includes purpose of the interconnection, relevant authorities, specify the responsibilities (downtime, billing, etc.), defines terms of the agreement (cost, etc.), termination/reconnection.
  + **Section 2: Cryptography**
    - Cryptography Basics
      * Cryptography is the process of taking data, providing confidentiality to that data, and then outputting it again. The practice of disguising information in a way that looks random.
      * Obfuscation: To take data that looks like it makes sense and hide it.
      * Diffusion: Making an image blurry or fuzzy.
      * Confusion: Making an image stirred up or non-sensical.
      * Encryption/decryption
        + Ceaser Cipher

Includes substitution. One of the earliest known and simplest ciphers.

Example:

WeAttackatDawn 
BJFYYFHPFYIFBS 
ROT S 

Easily decrypted with cryptanalysis.

* + - * + Vigenère Cipher

Like a Ceaser Cipher with more confusion involved.

Example:

OF A CEFACE FA CEFA 
We Attack at Dawn 
B E CXYAEO FT FEB N 
slr u 
; '10 s Tju 
'10 AIS' 
Tlu 

* + - * Classic cryptography components:
        + Algorithm
        + Key for encryption
      * Algorithms for binary data
        + Exclusive OR (XOR)

Example:

M 
{11010110 
01001101 
10011011 
10110101 
Θ1ΘΘ1ΘΘ1 
κ 
10101101 
01001011 
111ΘΘ11Θ 
01101011} 
β1ΘΘΘ1Θ1 
00101110 
lnput Output 
1 
1 
Ι 
1 
1 
1 

* + - * + Kerckhoffs' Principle

As long as you don't know what the key is to an encryption, you can understand the algorithm completely.

Today's algorithms are open standard.

By showing everyone the "lock", anyone can check the "lock" to see if it's pick-able.

Everyone knows the algorithm, but if you don't know the key, it doesn't do you any good.

* + - * Data at rest
        + Thumb drive, DVD, CD, etc.
      * Data in transit
        + VoIP call, text message, etc.
      * Data in process
        + Calculating in database where it is sitting in RAM/CPU.
      * Where do we encrypt/decrypt this data?
    - Cryptographic methods
      * Symmetric Encryption is where the same key is used to encrypt and decrypt a piece of data.
      * In-band keys are sent with the encrypted data.
      * Out-of-band keys have a key sent separately from the encrypted data.
      * Symmetric encryption is the primary way that we encrypt data.
      * Ephemeral key is a key that is temporary. Provides perfect forward secrecy.
      * When a key is setup in a way that knowledge of a key used in a previous session keeps someone able to crack encryption in a current session, that is called perfect forward secrecy.
      * Asymmetric encryption does not use a key. It uses a key pair.
        + Public key

Given to anybody

Only used to encrypt

* + - * + Private key

Kept by the sender of encrypted data

Only used to decrypt

* + - * Asymmetric encryption's big issue beyond key generations and exchanging, it is slow. It is mainly used to send a secure session key.
      * A cryptosystem is a highly defined piece of cryptography that programmers use to do their job and make cryptography work.
        + It defines key properties, communication requirements for the key exchange, and the actions taken through encryption/decryption.
    - Symmetric Cryptosystems
      * Algorithms have to be known to everybody, and it has to have a key of different lengths that are kept secret.
      * Symmetric Key Algorithms is defined by the same key used for encrypting/decrypting.
      * A Symmetric Block Algorithm continues to take defined blocks of data, encrypting that data, and continuing to repeat the process until all of the target data is encrypted.
      * Data Encryption Standard (DES) was invented primarily by IBM and is still used by the US Government.
        + 64-bit plain text
        + Initial Permutation - stirring of the data.
        + Key, has last 8 bits dropped, split into two 28-bit chunks.
        + The first 24-bits of each chunk is then combined to make a SubKey (48-bits).
      * The initial data has a Feistel Function performed
        + Take the 64-bits and split into 32-bit halves.
        + A 32-bit half is expanded to 48-bit using an Expansion function.
        + An XOR function is applied, using the SubKey.
        + S Boxes are used. Each S Box takes in 64-bits and outputs 4-bits.
        + 8 different S Boxes with a different 4-bit output.
        + Apply all S Boxes to the data, creating a 32-bit output.
        + A final permutation is performed, where the two 32-bit pieces of data are put together but backwards.
      * DES had issues with a short key. DES can be hacked in certain circumstances.
      * Two alternatives to DES: Blowfish, and 3DES (Triple DES).
      * Three things we look at regarding symmetric block encryptions.
        + Key size
        + Number of rounds
        + Block size
      * DES:
        + Block Cipher
        + 64-bit Block Size
        + 16 Rounds
        + Key Size: 56-bit
      * 3DES:
        + DES, but tripled.
        + Block Cipher
        + 64-bit Block Size
        + 16 Rounds
        + Key Size: 56-bit x 3 = 168-bit.
      * Blowfish
        + 64-bit Block Size
        + 16 Rounds
        + Key Size: Variable 32 to 448-bits.
      * AES
        + Advanced Encrypted Standard. Supported by NIST.
        + Symmetric Block Encryption
        + In essence, un-hackable.
        + Block Cipher
        + 128-bit Block Size
        + Key Size: 128, 192, or 256-bit.
        + Rounds: 10, 12, or 14.
      * A streaming cipher is where each bit is encrypted once at a time, in a pseudo-random manner.
        + RC4 is one of the only streaming ciphers. It is asymmetric.
        + Rivest Cipher 4 (RC4):

1-bit at a time.

1 round.

Key Size: Variable from 40 to 2048-bits.

* + - Symmetric Block Modes
      * Electronic Code Book (ECB) can create patterns by using the same key to encrypt blocks repeatedly. Always outputs same results with the same input.
        + This can apply to voice, data, anything that is encrypted.
      * A binary block is plain text converted into 16-bit, 64-bit, or 128-bit binary ciphertext.
      * We use different Block Modes to obfuscate the data better.
      * All Block Modes creates a chain of encryption.
      * The following Block Modes use an Initialization Vector, which ensures the output block is uniquely different.
        + Cipher Block Chaining (CBC)

Uses an Initialization Vector.

First block has XOR ran onto it.

* + - * + Cipher Feedback (CFB)

Uses an Initialization Vector, that is encrypted. The output of that encryption is XOR'd to the first block.

* + - * + Output Feedback

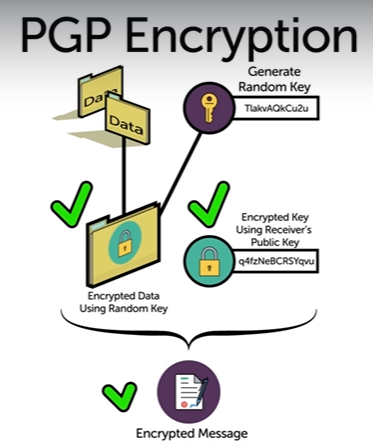
One Initialization Vector, encrypted, and the output is XOR'd to the first block. Same Initialization Vector continues to be used.

* + - * + Counter (CTR)

Uses a Nonce Value + Counter Value that continues to increment in binary. Then it is encrypted, and the first block of the plain text is XOR'd to create the first block of Cipher Text.

* + - * Nobody uses ECB anymore.
    - RSA Cryptosystems
      * RSA is an asymmetric algorithm.
      * Two large prime numbers multiplied together to form a semiprime number to generate a key pair.
      * Each public key has a single private key. Without the private key, the information can not be decrypted.
      * RSA includes protocols to authenticate the intended recipient.
      * RSA now uses a 2048-bit minimum for a key size in today's society.
      * ECC: Elliptic Curve Cryptography
        + Provides very small keys to transfer with the same robustness as large RSA keys.
        + ECC is based on an Elliptic Curve formula:



* + - * + Key pair can be plotted on elliptic curve.
    - Diffie-Hellman
      * An asymmetric algorithm, that is meant to provide a methodology for two parties to come up with the same session key.
      * Key Exchange (Agreement) Protocol
      * Diffie-Hellman Groups 
        Group I 
        Group 2 
        Group 5 
        Group 14 
        Group 19 
        Group 20 
        Group 21 
        768 bit modulus 
        1024-bit rmdulus 
        1536-bit modulus 
        2048-bit modulus 
        256-bit elliptic curve 
        384-bit elliptic curve 
        521-bit elliptic curve 
      * Subject to cracking due to large integers.
      * Groups help by defining the size or type of key structure to use.
    - PGP/GPG
      * Invented for e-mail encryption, originally.
      * Used to sign files, encrypt individual files, partition/disk encryption.
      * PGP uses the idea of a random key generated by the encryptor.
        + 
        + PGP Decryption 
          03 
          data key 
      * Public Key Infrastructure (PKI)
        + Certificate Authority 
          Intermediate 
          Authority 
          Individual 
          Users 
      * PGP Certificates
        + Symantec Corporation

Encrypts mass storage

Signing

Disk encryption

Bitlocker/Filevault

Designed for enterprise cloud solutions

* + - * + OpenPGP

Free

Open-source

Encrypted e-mail

PKI support

Works with S/MIME

* + - * + GPG (GNU Privacy Guard)

Free toolset

File and disk encryption

* + - Hashing
      * A hash provides integrity in regards to the CIA triad.
      * An algorithm that takes an arbitrarily large amount of data that runs through the hash, and comes out in a fixed value each time.
      * Hashes are one-way. Once a hash is generated, it is impossible to figure out what the original data was.
      * Hashes are used to verify sources.
      * Types of Hashes:
        + Message Digest 5 (MD5)

Invented 1992 by Ron Rivest

Uses 128-bit hash

Can create collisions.

* + - * + Secure Hash Algorithm (SHA)

Developed by National Institute of Standards

SHA-1 is the earliest type. 160-bit hash.

Can create collisions.

* + - * + SHA-256 (SHA-512)

Newer version of SHA with 256-bit or 512-bit hashes.

* + - * + RIPEMD (RACE Integrity Primitives Evaluation Message Digest)

Not very common.

Open standard

128, 160, 256, 320-bit versions.

* + - * Examples of hashes:
        + Password storage. Password saved as hash onto hard drive, not the plain text of the password.
        + Encryption and authentication
    - HMAC
      * Hash-based Message Authentication Code (HMAC)
      * Takes one individual packet and adds information to the end of that packet.
      * Generates hash, but not just a hash of the message; it also uses the key.
      * [www.freeformatter.com](http://www.freeformatter.com) has an HMAC generator/tester tool.
      * Provides message integrity.
      * Requires each side of the conversation to have the same key.
      * Based on standard hashes (MD5, SHA-1, etc.)
    - Steganography
      * Process and science of taking data and hiding it in other data.
      * The data itself may or not be encoded, but it is hidden in other data.
      * Text hidden within graphic images, most commonly.
      * Image Steganography: used to embeds data into .png, .jpeg, .bmp.
        + Tool used to input secret text into image.
        + In order to retrieve the data, the image must be decoded using the same tool by the recipient.
    - Certificates and Trust
      * HTTPS websites will send public key to your system.
      * Key exchange
        + How do we determine where the public key comes from? Or that it is legitimate?
        + Either key in a private and public pair can be the public key.
        + Different strings of ones and zeroes.
      * A digital signature is just a hash. A webpage has its entire webpage encrypted and sent to the client, and the client hashes it and compares the hash with the server.
      * A public key can have the originator's digital signature as well as a third party's attached to it, used to verify trustworthiness.
      * A digital certificate is a document that includes a public key, a digital signature from the generator, and the third party's digital signature.
        + Third parties create the digital certificate for the user.
      * Ways of trust:
        + Generate your own certificate

Unsigned certificate

* + - * + A web of trust requires maintenance and a lot of work.

This includes many end users certifying certificates.

* + - * + PKI (Public Key Infrastructure)

A hierarchal structure.

CA (Certificate Authority)

An organization that issues certificates.

Intermediate Certificate Authorities meant to load balance the CA's themselves.

Verisiqn 
VERISIGN• 
Thawte 
Paul 
Chris 
Richard 
Craiq 

* + Public Key Infrastructure
    - PLI is a trust model.
    - The infrastructure that we use for every real world application that uses public keys/digital certificates.
    - Root certificate is the top of the hierarchy, distributes certificates to intermediate systems.
    - PKI is NOT a standard.
    - PKCS is the de facto "standard" for most systems.
      * Public Key Cryptography Standards = PKCS
    - PKI is based off of X.509, which defines organization through hierarchy to access data on a timely basis.
    - PKCS #7 is used to export certificates to an individual without private keys.
    - PKCS #12 is used to export certificates with private keys encrypted within it as a package.
    - CRL (Certificate Revocation List) Distribution Points
      * Gives your system the opportunity to audit trail the certificate.
      * CRLs can take up to 24-hours to react to "bad" certificates.
        + An expired certificate is not a "bad" certificate.
    - Since CRLs take so long, the modern era uses OCSP (Online Certificate Status Protocol).
      * OCSP is real-time in terms of checking if a certificate is bad.
  + Cryptographic Attacks
    - Interpreted as cracking passwords.
    - Passwords are traditionally hashed.
    - Password attacks are typically cracking hashes.
    - One of the hardest aspects of attacking is how to get into a server or system in which passwords are stored.
    - If the password is stored in a hash, there's no way to reverse the hash.
      * Hashing attacks are comparative attacks. Generating hashes over and over until one matches the hash found.
    - Brute Force Attack is when a hash is put into a program and ran repeatedly to generate a match.
      * Takes a lengthy amount of time.
      * Generating, based on predefined character range, hashes to find a match.
    - Dictionary Attack uses a text file with dictionary words that manipulates them in an attempt to crack commonly-used human passwords.
      * Text files with hundreds of thousands of dictionary words can be downloaded and used to reference in an attack.
      * Takes advantage of the fact that human beings use words they are familiar with for passwords.
    - Rainbow-Table Attack
      * A rainbow-table is a pre-generated bunch of hashes.
        + An indexed hash table.
        + Uses reduction formula.
        + Already has hashes in it.
        + A rainbow-table is massive. Small rainbow tables are over 10GB.
      * A hash table is nothing more than a bunch of words with a hash in it.
    - Most good password storage obfuscates the password hash to make it harder to crack.
      * OpenSSH, for example, adds two random bytes to the end of a password hash.
    - Salt
      * An arbitrary value
      * A salt situation example:
        + Password = Timmy
        + Password with salt 3456 = Timmy3456
        + This means that the password is altered BEFORE it is hashed.
      * Salted hash tables are very hard to crack.
    - With wireless, key stretching is used.
      * A passphrase and SSID together generates a combined hash that is much harder to crack.
      * WPA for wireless uses PBKDF2
      * Key stretching technique - bcrypt
      * Proper key stretching is basically unhackable, with proper password precautions.
    - Complex passwords are used to make cryptographic attacks harder.
  + **Section 3: Identity and Access Management**
    - Identification
      * Identification, Authorization, Authentication
        + Identification just proves who the user is to the authenticating systems.
        + Authentication is the user proving they have rights to that system.
        + Authorization is what rights the user has to the system once authenticated.
      * Authentication Factors
        + Something you know.

Passwords, PIN codes, CAPTCHA, security questions.

* + - * + Something you have.

Smart card.

Embedded somewhere on the smart card has a chip with a unique identifying code.

RSA key (token)

Can be software based or hardware based.

Stores a secret code of some form.

Generates a value that changes every so often.

* + - * + Something about you.

Retinal scanners. Finger print scanners. Iris patterns.

* + - * + Something you do.

Rhythm of typing, typing style.

* + - * + Somewhere you are.

A credit/debit card detecting an interaction out-of-state, entering zip code for gas station.

* + - * Federated Trust
        + Trust inherited from a different trusted system.
        + Used in Windows Active Directory
        + Domains trusting other domains
      * Multi-factor Authentication (2FA/MFA)
        + Fingerprint scanner + username and password.
        + Password + hardware token.
    - Authorization Concepts
      * Authentication is used to access a system, while authorization is used to determine what a user can do within a system.
      * Concepts:
        + Permissions

What are the things assigned to a user?

Administrators assign permissions

Groups/OUs are often assigned permissions as opposed to individual users.

* + - * + Rights/Privileges

Rights or privileges are assigned to systems as a whole.

Do you have the right to change your password, or desktop wallpaper?

* + - * + Least Privilege/Separation of Duties

Least privilege always says give your users the least amount of privilege to get their jobs done.

Separation of Duties

Keeping different people, groups, and permissions separated from conflict of interest areas.

* + - Access Control List (ACL)
      * Authorization Models
        + How over time have we developed the concepts of authorization?
        + Mandatory Access Control (MAC)

Label-based

"Secret/Top Secret" clearances

Classified/Unclassified

* + - * + Discretionary Access Control (DAC)

Whoever created the resource is the owner/creator

The creator/owner defines access/permissions

* + - * + Role-based Access Control

Applies access controls to a resource by a role.

Used by most all modern operating systems.

Groups are used to define roles.

* + - * + Any good ACL will have an implicit deny.

An implicit deny is unless you specifically allow something to happen, it isn't going to happen.

* + - * + Anything that needs to control access will have an ACL.
    - Password Security
      * An example of a good security policy:
        + Complexity - Length and character requirements
        + Expiration or age - Reset and time triggers
        + Password History - Reusage and retention
      * GPOs can be used to create password security requirements applied within domains.
        + Also can be applied to sites, groups, OUs.
        + GPOs are only used within a Windows AD environment.
    - Linux File Permissions
      * File and folder permissions
        + ls -l lists permissions within a directory.
        + Group 
          rwxrwxrwx 
          Owner 
          Everyone 
        + R = Read

Opens a file, or views contents of a directory.

* + - * + W = Write

Edit a file, or add/delete files within a directory.

* + - * + X = Execute

Run a file, or change to a different directory.

* + - * + chmod = short for change mode

Command example: chmod o= RunMe

Changes permission for others to have no rights, on the file RunMe.

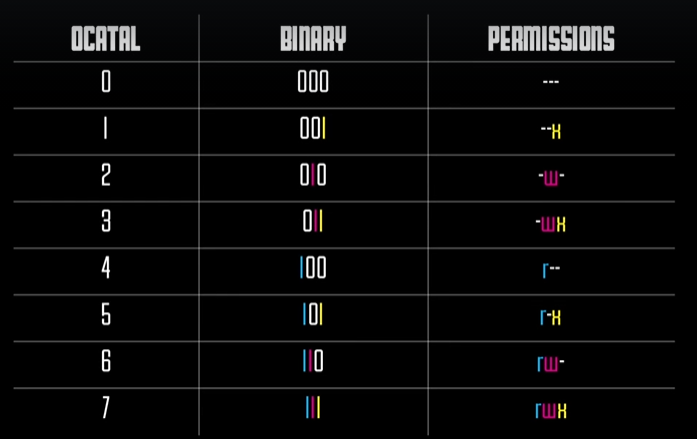
Command example: chmod g=rx RunMe

Changes permission for group to have read/execute permissions, on the file RunMe.

Command example: chmod a=rwx RunMe

Changes permission for all to have read/write/execute permissions, on the file RunMe.

chmod can be used with binary/numbers instead of letters.



* + 
  + chown is used to change ownership
    - Needs sudo to work.
    - Command example: sudo chown root RunMe
      * Changing the owner to root for the file RunMe.
  + passwd is used to change users password
    - Needs sudo to work.
      * Command example: sudo passwd
        + Changes password on logged in account. Requires the new password to be typed in and confirmed.
  + Windows File Permissions
    - NTFS Permissions
      * Read & execute is for running files.
      * Read is only for viewing data files.
      * Full control is allowing all permissions.
      * List folder contents is where the files can be viewed directly, but the user (without the permission) cannot view the files within the parent folder.
      * Modify is for editing/saving files within the folder.
    - The best practice is following:
      * Create users, put the users into groups, and then permissions are put onto folders in terms of groups.
    - Inheritance
      * When NTFS permissions are set for an object, anything created within that object receives those permissions.
    - Copying and moving objects within NTFS formatted partitions
      * Copy from source drive will take on the NTFS permissions of the destination drive.
      * Copying within the same drive will lose its NTFS permissions.
      * Moving within the same with will keep its NTFS permissions.
  + User Account Management
    - Continuous Access Monitoring
      * Monitor 24/7 what users are able to get into.
      * Track log on/log off activity.
      * Track file access.
    - Shared Accounts
      * Shared accounts are bad.
      * Biggest example is a workgroup with one account on each machine.
      * Don't share accounts.
    - Multiple Accounts (for one user)
      * Sometimes is a necessity.
      * If it happens, use different usernames/passwords across the accounts.
      * Use different groups. Monitor which users belong with which groups.
      * Use least privilege - enough necessary to complete a task.
      * If you give someone a second account with elevated privileges, make sure they only use that account for what is necessary and then log off.
      * Monitor and log activity of users with multiple accounts.
    - Default and Generic Usernames/Passwords
      * Use dedicated service accounts.
        + Makes it easy to log and track.
  + AAA
    - Authentication, Authorization, and Accounting (AAA)
      * Remote Authentication Dial-In User Service (RADIUS)
        + Designed to support Dial-in Networking.
        + Uses RADIUS server within a LAN that is trying to be accessed.
        + A RADIUS client is the gateway being used.
        + A RADIUS Supplicant is the system trying to be authenticated.

Supplicant -> RADIUS Client -> RADIUS server

* + - * + Used for wireless authentication (mainly corporate networks)

Every wireless access point can be used as a RADIUS client to send off to a RADIUS server for authentication.

* + - * + Mainly used for network access.
        + Can use 4 UDP ports:

1812

1813

1645

1646

* + - * + Does not handle authorization, only authorization.
    - Terminal Access Controller Access-Control System Plus (TACACS+)
      * Form of AAA
      * Proficient at managing a bunch of devices.
      * Takes care of the authorization aspect.
      * Decouples authorization from the authentication.
      * Once you are in (authorization), it defines in real time what you can do (authentication).
      * Uses TCP port 49.
    - Both TACACS+ and RADIUS do auditing (accounting) for log files.
  + Authentication Methods
    - The process of Authentication requires encryption.
    - Password Authentication Protocol (PAP)
      * Oldest authentication method.
      * Client system sends username/password in clear text to server system.
    - Challenge-Handshake Authentication Protocol (CHAP)
      * First authentication protocol used in the PC world to protect authentication process.
      * Server and client have password key stored in them.
      * Client system sends "May I authenticate?" message to the server, in which the server makes a "Challenge Message" of the two keys (hashed). The client then generates the same hash and is sent to the server.
      * No passwords being passed, only hashes.
    - NT LAN Manager (NTLM)
      * Isn't used in advanced Windows authentication methods.
      * Still used with Windows systems in a workgroup.
      * Currently NTLM v2.
      * Starts initial hello between client and server, and then each side takes a challenge message (which is hashed), and challenge message each other.
      * Similar to a double CHAP.
    - Kerberos
      * Only used in authenticating to Windows domain controllers.
      * Domain controller is known as the Key Distribution Center (KDC).
        + Authentication service
        + Ticket granting service
        + Use TCP/UDP Port 88
        + Ticket Granting Ticket (TGT) shows that user is authenticated to the domain. Also knows as SID (Security Identifier) Not authorized at this point.
        + TGT generates a Session Key is what authorizes what resources the user can access. If the user wants to go anywhere else on the domain, a new session key is generation.
    - Security Assertion Markup Language (SAML) and Lightweight Directory Access Protocol (LDAP)
      * Neither one of these are authentication methods, but similar.
      * SAML is used exclusively for web applications.
      * LDAP is used to access someone else's directory. A structured language used to allow one computer to go into someone else's directory.
        + Main process to access file resources in Windows is based on LDAP.
        + TCP/UDP port 389.
  + Single Sign-On (SSO)
    - LAN uses Windows Active Directory for SSO tools.
      * Once a domain is established, the client PCs join the domain.
      * Once this is established, a trust situation and federated system is established.
    - Security Assertion Markup Language (SAML)
      * Designed for web applications.
      * Allows a single person in a single place to log onto multiple devices.
      * Starts with having an Identity Provider (IP).
        + Once a user signs onto an Identify Provider, all of the connected applications are called Service Providers.
        + The IP provides a token to log onto all the individual devices (service providers).
    - What type of security needs will be necessary?
      * Example: A local area network for folders/files will need Windows AD.
      * Example: Any wide area networks/public items will need SAML.
  + **Section 4: Tools of the Trade**
    - OS Utilities Part 1:
      * ping
        + Used often to checking DNS, such as pinging a FQDN to check if it replies. If it replies, it shows DNS is working.
        + Used to check if an IP address can be connected to.
        + -4 is a switch used to make the command only respond in IPv4.
        + Used to check hardware/network issues and intermittent connection with the switch -t for a persistent ping.
        + Linux does not need a -t as it always uses a persistent ping.
      * netstat
        + Used to check sessions a computer has open.
        + -n displays addresses and port numbers.
        + -a displays hosted server ports.
      * tracert
        + If the trace route fails on the first two hops (internal router and machine interface) that shows the issue is in-house.
        + Everything after the second hop is ISP-related.
      * ARP
        + Address Resolution Protocol. Used to resolve ethernet MAC address from an IP address.
        + arp -a command shows cached ARP table.
        + Windows generations static ARP entries.
        + Dynamic ARP entries change based off ARP commands that the host picks up.
    - OS Utilities Part 2:
      * ipconfig
        + Ipconfig /all displays all data for "Who am I?"
        + Typically best server used in a known network.
        + -all finds MAC address.
      * ip addr
        + Linux command. Not used in Windows.
        + Ifconfig is depreciated.
      * nslookup
        + DNS servers have learned to not respond to these queries since they are exploited so often.
        + nslookup [www.google.com](http://www.google.com)

Makes query "What server am I using for DNS?" and the IP address of that server.

Running nslookup in interactive mode and changing the DNS server to another can be used to troubleshoot issues.

* + - * digg
        + Used in Linux, not Windows.
        + Also checks DNS entries similar to nslookup.
        + @192.168.0.1 added will change DNS server to the IP address.
        + dig mx google.com will query MX record of the website.
      * netcat
        + Can open/listen on ports, and can open/act as a client on any port.
        + Tool for aggressive use.
    - Network Scanners
      * Can be used to detect open ports, protocols, hardware and rogue systems.
      * Resource intensive, and intrusion prevention systems will be alerted.
      * Nmap
        + Useful for hardware inventory and reconnaissance.
        + nmap -v -sn 192.168.0.0/24

Searched local network for IP addresses and what they correspond to.

* + - * + Nmap -v -A scanme.nmap.org

Verbose output, -A symbolizes listing operating systems.

Discovers open ports.

* + - * + Zenmap is a GUI that runs nmap. It comes with the nmap download.
      * Wireshark SB Network Inventory

* + Protocol Analyzers
    - Used to analyze network traffic in/out of specific host computer.
    - Any protocol analyzer has two main sections:
      * Sniffer
        + Like pcap, tools that actually grab data going out of a particular interface.
      * Analyzer
        + Reads pcap data, and analyzes/formats it in a way we can read.
    - Wireshark
      * Free and powerful tool used to scan network traffic.
      * Filters data by services and protocols.
      * Displays tremendous amount of information.
        + Information can be filtered by categories.
      * Helps find Broadcast Storms
        + When a NIC breaks and begins broadcasting huge amount of data.
      * Can be used with different sniffers than what comes with it.
        + An often-used one is TCPDump, which runs only on Linux.
  + SNMP
    - Simple Network Management Protocol
    - A tool which allows administration and management of network devices from a single source.
    - Ports UDP 161 (unencrypted) and TLS 10161 (encrypted) are the ports the agent of the device listens on.
    - An SNMP Manager is the system that manages the managed devices.
    - A Network Management Station (NMS) is an SNMP Manager with the proper SNMP management software on it.
      * An NMS uses ports UDP 162 and TLS 10162 for listening.
    - Management Information Base (MIB) is a factory built-in database within a device that can be queried for communication.
    - Types of communication/queries:
      * Get
        + NMS sents "get" to managed device, in which the managed device sends a response.
      * Trap
        + Set up on the managed devices themselves.
        + A "trap" is set once a value meets a threshold.
      * Walk
        + Batch process of "gets".
        + More commonly referred to as SNMPWalk.
    - SNMP has three versions.
      * Version 1:
        + First version with a limited command set, no supported encryption.
      * Version 2:
        + Uses basic encryption, slightly expanded command set.
      * Version 3:
        + Uses TLS encryption.
    - An SNMP community is an organization of managed devices.
    - Read Only (RO) vs. Read Write (RW) can be added on the command to turn on the SNMP service.
    - Cacti is an open-source NMS for graphing SNMP data.
      * Nagios, Zabbix, and Spiceworks are also NMS brands.
  + Logs
    - Event logs, security logs, device logs, audit logs.
    - Exist anywhere on a system, depending on the system.
    - Non-Network and Network Logs
      * Non-Network Events happen on a host even though it's not connected to a network.
      * Typically have a date or time, process/source, account, event number, description.
        + Operating System Events

Starting, shutdown, updates, service events.

* + - * + Application Events

Application installation, stop/start/crash

* + - * + Security Events

Logons, success/failure.

* + - * Network Events deal with the communication between the host and network.
        + OS/system-level events

Remote logons (fail/success)

* + - * + Application-level events

Activity on web server, firewall.

* + - * Decentralized Logging is where each host has its own set of logs.
      * Centralized Logging uses a central repository, which can cause a drag on the network.
        + SNMP systems are utilized here.
        + Third-parties Monitoring as a Service (MaaS) are sourced for this often.
  + **Section 5: Securing Individual Systems**
    - Denial of Service
      * Designed to deny service in some form.
      * Types of DoS Attacks:
        + Volume attack

Ping floods

UDP floods

* + - * + Protocol attack

SYN flood/TCP SYN attack

Client continues sending SYN repeatedly with client never responding with SYN/ACK.

* + - * + Application attack

Slow Loris Attack

Client initiates conversation, and does not give a response. Client continues initiating conversations without a response.

* + - * + Amplification Attack

Smurf attack

Attacker spoofs IP address, sending out an ICMP which causes all clients on the network to respond to a spoofed target.

* + - * Distributed Denial-of-Service Attacks (DDoS)
        + Uses multiple systems to attack a host.
        + Typically a BotNet (malware) is deployed.
        + Client machines infected with malware (zombies) report to a single machine controlling them all.
    - Host Threats
      * Spam
        + Unsolicited e-mail. Normally not considered a threat, but more of an irritant.
      * Phishing
        + Simply spam but trying to obtain information from you.
        + Spear phishing obtains personal information before contacting you for more, such as name.
      * Whaling
        + Phishing targeting a high-level employee.
      * Spim
        + To receive spam via instant messaging.
        + Again, more of an irritant.
      * Vishing
        + Unsolicited use of voice to obtain information.
      * Clickjacking
        + When a website tricks you into clicking somewhere you didn't intend.
        + Typically referred to authorizing something, such as a download.
      * Typo Squatting & Domain Hijacking
        + Typo Squatting takes advantage of people mistyping URLs.

People buy domains and websites hoping people make typos.

* + - * + Domain Hijacking

When a domain expires and someone buys that domain quickly to put offensive or obscene content on it, then contacts you to buy it back from them.

* + - * Privilege Elevation
        + Not truly a threat, but listed as one on the test.
    - Man-in-the-Middle
      * On any TCP/IP network, communication exists between two computers. A third party sneaking between this communication is a Man-in-the-Middle Attack.
      * Uses the information to the third party's advantage.
      * Wireless communications (802.11 WiFi, Bluetooth, NFC) are susceptible to Man-in-the-Middle attacks.
        + Encryption is needed within wireless.
      * Wired Man-in-the-Middle Attacks often require IP or MAC address spoofing to trick networks to sending the attacker its information.
      * MAC Spoofing = Port Stealing
      * ARP Poisoning = IP Spoofing
      * The number one reason for deploying a Man-in-the-Middle attack is to gather data.
      * Replay Attack is best used for secure connections.
        + By obtaining the username and password hash, you can "replay" that information to the server to log in.
      * Downgrade Attack is querying a web server for a lesser protocol version, and then exploiting that weaker protocol.
      * Session Hijacking is getting in the middle and injecting information of a current open session between machines in real time.
    - System Resiliency
      * Scalability
        + Adding more of a resource to service demand.
      * Elasticity
        + Going from a large amount of resources to a smaller amount as needed to fit demand that changes.
      * Redundancy
        + More than one of the exact same thing for failover purposes.
        + Doesn't define much more than having more than one.
      * Distributive Allocation
        + Having redundancy in terms of multiple locations - such as offsite backups, or servers in different locations.
      * Non-Persistence
        + Not persistent/permanent.
        + Snapshot - Take the current state of an item, on a binary level, and saving it as a backup/copy.
        + Known state - While a snapshot talks about an entire machine, a known state is referencing one aspect of a machine.

Windows Update is an example, where reverting to a type of system build (Windows 10.x.x) is used to fix the state of a machine.

Configuration files for networking devices is another example.

* + - * + Rollback

Tends to zero in on a very small part of a system, such as Windows drivers.

* + - * + Live-CD

Not limited to only a CD, also a thumb drive or any bootable media.

You can boot into an OS off of the media and "try" something on that instead of writing to a hard drive.

* + - RAID (Random Array of Independent Devices)
      * Primary way that we provide security to stored data.
      * Instead of using one hard drive, use multiple hard drives to work together as one hard drive.
      * Provides integrity and improves data access, or both.
      * Types of RAID:
        + RAID 0

Known as striping.

Designed to increase data speed, provides no data integrity.

Disperses data across multiple drives.

Minimum of two drives.

Downside to striping is that losing any drive means the data is lost.

* + - * + RAID 1

Requires an even number of drives.

Known as mirroring.

Provides data integrity with no speed increase (actually slows things down)

* + - * + RAID 2

Minimum of three drives.

Data is saved in sections on two drives and the third drive (dedicated parity drive) saves the parity equation to it.

RAID 2-4 uses two or more data drives that store individual pieces of data (stripes) and then a dedicated drive that only handles parity.

* + - * + RAID 5

Minimum of three drives.

Parity is spread out across all drives.

Downside is that one drive can be lost, but more than one drive cannot be lost.

Was the most popular RAID configuration for a long time.

* + - * + RAID 6

Minimum of four drives.

Two parities are created, therefore two drives could be lost without data loss.

* + - * + Raid 0+1

Referred to as RAID 01, it is a mirror of stripes.

Two hard drives working as one mirror, two hard drives working as the other side of the mirror.

One data mirrored to both drives, striped on both drives.

Generating a mirror of stripes.

* + - * + RAID 1+0

Referred to as RAID 10.

Data is striped and mirrored on each drive.

* + - * + Proprietary RAID

A big issue with established RAID levels is waste.

RAID 5 for example requires same size drives for all drives, otherwise the bigger drives will have their sizes reduced to meet the smallest.

Companies such as Synology have proprietary RAID configurations.

* + - NAS and SAN
      * Network Attached Storage
        + File-based sharing protocol.
        + File-level.

RAID arrays, formatted and partitioned, treated as a network share like Samba.

* + - * + Usually running some type of OS.
        + Runs over a standard network, using TCP/IP.
        + Uses well-known protocols, showing as shares on a network.
        + Used often in small workgroups.
      * Storage Area Networking
        + Relies on some kind of technology to transfer data between systems and storage.
        + Work on the block-level.

Considered "Block-level storage".

* + - * + The best SANs use Fibre Channel

Fibre Channel (FC) is its own network to move data around.

Requires Host Bus Adapter (HBA) into computer.

Fibre Channel switch connects to Fibre Channel Controller on a SAN.

* + - * + Poor man's version of SAN is called iSCSI

Uses existing network, interconnecting to different devices - showing as a physical hard drive (block-level)

Initiator and Target - terms used in an iSCSI network.

Initiator looks for targets and makes the target one of its hard drives.

Once a target is made, the Extent of that target has to be made.

Once the target and extent is put together into a group with a LUN ID, it is able to be accessed via iSCSI initiator.

* + - Physical Hardening
      * Removable Media Controls
        + Not referring to USB. Refers to optical media.
        + CD/DVD
        + Local computer policies can dictate what users are able to do with their removable media.

Can be configured system-wide or user-based.

* + - * Data Execution Prevention (DEP)
        + Used to be a problem where programs could be executed in memory that isn't supposed to be accessed.
        + Under System > Advanced System Settings > Performance in Windows, DEP can be turned on/off.
        + DEP should always be turned on.
      * Disabling Ports
        + BIOS/UEFI can have specific ports turned off.
        + USBs can be turned off as a whole depending on the motherboard's BIOS/UEFI.
        + USB Mass Storage Driver Support can be turned off, which means devices such as keyboards/mouse will work but drives which transfer data will not.
        + Serial/Parallel ports can be turned off as well, among others.
    - RFI, EMI, and ESD
      * Electromagnetic Interference
        + AKA Electromagnetic Pulse
        + When radiation of a device interferes with other devices as a whole.
      * Radio Frequency Interference
        + Radiation interfering with devices in the radio range, like wireless access ports.
      * Electrostatic Discharge
        + Based on electricity.
        + Staying at the same potential to avoid charges.
      * Ways to protect against the above:
        + Isolate - move devices away from each other.
        + Shield - shielded ethernet cable.
        + Separate circuits - keeping currents on different circuits.
    - Host Hardening
      * Disabling Services
        + Going through process of disabling unnecessary services.
        + Some programs also do not have an interface or service running on them, but they act as a service.

For example, a machine running a web server or SSH server, do those need to be running?

This is technically not a service but essentially is.

* + - * Default Passwords
        + Typically Internet of Things (IoT) devices have default passwords turned on, which is the biggest issue with botnets.
      * Disabling Unnecessary Accounts
        + Domain Groups and Domain Users within those groups are unnecessary.
        + Having multiple groups or accounts with the same privileges/permissions instead of one bottleneck is an issue.
        + Too much group/user division can create attack surfaces.
      * Patch Management
        + Any modern OS has patches/updates.

This applies to any type of device. Switches, desktops, cameras, etc.

* + - * + Patch Management Steps:

Monitor - Monitor new patches and their implications.

Small devices may not get reminders or automatic updates.

Test - Use a sandbox environment to test first before deploying.

Evaluate - Is this an important patch? Does this apply to us?

Deploy - Deploy the patch. Schedule the process in large environments.

Document - Take note of what patches have gone out/been skipped and their consequences.

* + - * Anti-Malware
        + Keep Anti-Malware as updated as possible.
        + Train users, as they are the number one line of defense.
        + Procedures should be in place once users encounter and recognize anti-malware.
        + Recognize and enforce good practices.
        + Monitor security logs, network flow diagrams, check DNS logs.
        + Intrusion Detection Systems (IDS) could be used as well.
      * Host Firewalls
        + Every computer in the network should have a host firewall.
        + Firewalls work on an application-level basis.
        + Enterprise environments should have white/blacklisted applications.
        + Centralized Management Tools should apply here in order to keep things tight and not allow users to alter any policy.
    - Data and System Security
      * Data Security
        + Data integrity
        + Speed/quick access
        + High availability

Types of Data Security:

RAID

Provides integrity

Provides speed

Affordable

Only applies to drives/storage within a system.

Clustering

Simply means having more than one computer doing the same job, sharing resources/data.

If one system dies, the other kicks in and takes its spot.

The downside is each computer has to keep the other one updated.

Very expensive. One cluster machine typically does the work, while the others are backups.

Load balancing can also take place with clustering.

Workload distributed across clustered servers.

Virtualization

If one server were to "die" or become corrupted, a snapshot can simply be spun up to remedy the issue.

* + - Disk Encryption
      * Encrypts data stored on mass storage.
      * Can slow systems down, such as a large file server.
      * Disk Encryption Usage
        + Mobile and portable devices.

Laptops, smartphones, tablets.

* + - * + Desktop systems with limited security.
      * All encryption tools can be broken into two camps:
        + Trusted Platform Module (TPM)

A TPM chip that houses a public private key.

The private key cannot be removed from the TPM.

A hard drive encrypted with a TPM, for example, cannot be decrypted unless it is connected to the TPM chip.

* + - * + Non-TMP Platforms
      * Activating TPMs often are done at the BIOS level.
      * PGP (Pretty Good Privacy) disk, TrueCrypt, BitLocker are all examples of encryption tools.
      * The recovery key must be recorded in some fashion, as the encrypted data cannot be viewed without it.
    - Hardware/Firmware Security
      * Full Disk Encryption (FDE)
        + Best security for mass storage is to encrypt it.
        + Software or firmware-based tools are typically discussed here.
        + BitLocker takes advantage of TPM.

The TPM has to be turned on in order for BitLocker to run.

* + - * + A recovery key must be documented in order to prevent data loss in the event of a motherboard dying.
      * Self-Encrypting Drive (SED)
        + A hard drive that has a TPM module built-in, which requires a password to be applied to the hard drive. Upon boot, the password must be entered to "unlock" the drive and boot.
      * Secure Boot
        + TPM 2.0 includes Secure Boot.
        + The OS will check the quality of all encompassing firmware and applications for signatures.
        + Secure Boot establishes the following:

Hardware Root of Trust

Secure Supply Chain

* + - * Hardware Security Module (HSM)
        + A HSM's only job is to calculate and check signage, store keys, etc. to make sure everything on a system is secure.
    - Secure OS Types
      * What type of OS do I use in a particular situation?
      * Server OS: An OS version designed to support servers.
        + More hardware support, programs (DNS, DHCP, AD), support for server software, etc.
      * Workstation (Desktop) OS: Windows 10, Ubuntu, Mac OS.
        + Workhorse systems, good network functionality, good support for hardware, doesn't support full-blown RAID.
      * Embedded Systems: Routers, cameras, doorbells.
        + Individual devices that cannot be built-upon. No screen, keyboard, mouse.
        + Full-blown computers running operating systems.
        + Come with their own OS.
      * Kiosk: Some big screen (touch screen) with customized interfaces to display.
        + Slimmed-down versions of Linux.
        + A few dedicated Kiosk operating systems.
      * Mobile OS: Mainly iOS or Android.
        + Custom designed for smart devices such as phones and tablets.
        + Provides a good level of security compared to Windows 10.
      * Which OS has the least functionality but enough to do the job that it needs to do?
      * Any OS has a high degree of security, but some operating systems are set up for specifically security
        + Trusted Operating Systems, made by the Secure Computing Group, are operating systems certified (often for the government) to be at the highest level of current security.
    - Securing Peripherals
      * Wired vs. wireless peripherals
        + Blue Jacking

Rare today

Definition: Connecting to Bluetooth device to use.

* + - * + Bluesnarfing

Connecting to a Bluetooth device to steal data.

Grabbing and stealing data is bluesnarfing.

* + - * + Bluetooth comes in three different classes.

Class 1: 328' connection distance.

Class 2: 33' connection distance.

Most phones, headsets are this class.

Class 3: 3" connection distance.

* + - * + 802.11 feature WPS is used on some devices.

WPS is Wi-Fi Protected Setup

Press WPS button on device, press WPS button on router, and they will automatically connect.

WPS is insecure and a big problem.

* + - * + Hidden Wi-Fi

Many devices have SD slots, and attackers will use Wi-Fi SD NICs to plug into these devices' SD card slots to take data.

* + - * + Displays/Monitors

Relatively secure devices, with the exception of the USB ports on the device.

* + - * + Think about what you are buying. Are these SD card slots or USB port necessary? Turn off unneeded ports. Don't forget peripherals need patches and updates too.
    - Malware
      * Nothing more than malicious software running on your system.
      * Types of Malware:
        + Virus

Piece of software that is placed on your system and attach to other files, then propagate itself to other media and spread.

Activates execution, like removing files.

* + - * + Adware

Programs that try to put ads up. Web-centric.

* + - * + Spyware

Some form of malware hiding from you that reaches out to a central location.

* + - * + Trojan Horse/RATs

Trojan is a piece of software that runs on a system that is compelling to have been downloaded, that is malicious.

Remote Access Trojans (RATs) aren't malicious until someone in a remote location turns it on.

* + - * + Ransomware/Crypto-malware

Locks the system files/encrypts them in order to extort money.

* + - * + Logic Bomb

Similar to a RAT.

Program sitting on a computer that has to be activated, but is triggered by an event.

* + - * + Rootkit/Backdoor

A rootkit grabs admin privileges to propagate to other pieces of a system. Notorious to detect.

A backdoor is a piece of software that has an intention to be accessed again.

* + - * + Polymorphic Malware

Malware that changes itself. Anti-Malware programs use digital signatures, and polymorphic viruses change their digital signature to avoid detection.

An armored virus is designed to make it hard for the anti-malware to recognize.

* + - * + Keylogger

Records key strokes to capture data/information.

* + - Analyzing Output
      * Anti-Malware/Anti-Virus
        + Check logs for virus type and location on program.
        + Can compare on databases.
        + All software these days update definition databases automatically.
      * Host-Based Firewalls
        + Any firewall installed on an individual host.
        + Access Control List (ACL)/Rules List.
      * File Integrity
        + Can be system-based, application-based.
        + Checks file versions, dates, names.
      * Application Whitelist
        + Their job is to make sure everyone is running a standard program/version/application on individual enterprise systems.
    - IDS and IPS
      * The firewall is the first line of defense.
      * Firewalls are imperfect, which is where Intrusion Detection Systems on the inside of the network come into play.
      * An IDS watches internal network traffic and sends alerts on suspicious activity.
      * An IDS can be software on a machine or a network appliance.
      * Once IDS became "active" where it began communication with the firewall to take action, is called Intrusion Prevention System (IPS).
    - Automation Strategies
      * Automation makes repetitive tasks easier.
      * Automation is consistent.
      * Template restoration is a scenario in which automation is important. Applying the same base image to all machines in an enterprise.
      * Continuous monitoring is a scenario in which automation is important. SNMP, for example.
      * Windows Update is an example of automation.
      * Monitoring application whitelists - automating continuous monitoring on hosts for application whitelisting and installations.
      * Automated application development is used widely in a modern sense.
      * Built-in Tools vs. Shells
        + Most modern OS's have shells, like PowerShell.
    - Data Destruction
      * Media Sanitation is another term for Data Destruction - they are synonymous.
      * Three levels:
        + Clearing

Use some internal command within the mass storage device to erase data from the media.

Example: An erase command on the HDD.

* + - * + Wiping

Begins at the beginning of the drive to the end of the drive, writing random binary to remove all data.

* + - * + Purge

To do something to the device, externally, to make the data go away.

Crypto Erase

Destroying the keys for the encrypted drive, which in essence purges the drive because it's useless.

* + - * + Destroy

To ruin the media in such a way that it is no longer functional.

Paper media, tape media, floppy disks.

Burning, pulping (soak in water, grind it up), shredding, pulverizing.

* + **Section 6: The Basic LAN**
    - LAN Review
      * Switches
        + Filter and forward data based on layer 2 (MAC addresses)
        + VLAN

Virtual LAN

Splitting single broadcast domain into multiple broadcast domains.

Layer 2 separation of networks.

* + - * + Flood Guarding

Also known as Spanning Tree Protocol (STP).

Prevents floods or loops.

* + - * Router
        + Filter and forward based on layer 3 (IP addresses)
        + Gateway router (interface between internet and network) will always run NAT.
      * Firewall
        + Piece of software commonly run on a gateway router for security purposes.
    - Network Topologies Review
      * Local Area Network (LAN)
        + All computers on a broadcast domain.
        + A broadcast domain is when individual computers sends out a broadcast, all other computers that hear that broadcast are on a broadcast domain.
      * Wide Area Network (WAN)
        + Local Area Networks connected together with routers between them creates a Wide Area Network.
        + WANs can connect to one another.
      * Metropolitan Area Network (MAN)
        + Multiple WANs that span entire cities.
      * The protocol which runs the internet is TCP/IP.
      * Intranet is a private network which still runs on TCP/IP.
      * Extranet is a private connection into an intranet.
  + Network Zone Review
    - DMZ (Demilitarized Zone)
      * Usage of two different routers in between the LAN and internet.
      * Demilitarized Zone (DMZ) 
        Local Area Network (LAN) 
    - Wireless Networks
      * A wireless connection is essentially the same as plugging in ethernet from a switch.
      * Guest Networks - Does not have LAN zone access. Separate VLAN.
    - Virtualization
      * Using a virtualized network.
    - Air Gap
      * Two LANs with a disconnect between them to provide real isolation to each LAN.
  + Network Access Controls
    - Wireless access
    - Remote access
    - VPN access
    - These cases have some form of system acting as a gatekeeper to allow you to become a part of the target network.
    - This started with Point-to-Point Protocol (PPP) which was designed for dial-up networks.
      * Designed primarily to take a computer with a phone line to connect to a service provider.
      * Transport layer protocol
        + Initiates connection
        + Obtain address information
        + Make connection
      * Had very rudimentary authentication methods
        + Password Authentication Protocol (PAP)

Passwords in clear text

* + - * + Challenge Handshake Authentication Protocol (CHAP)

Comparing hashes after a target creates a challenge.

* + - * Extensible Authentication Protocol (EAP)
        + More of a framework designed to run inside transport layer protocols, handling strictly authentication.
        + Was developed initially as an extension for just the authentication portion of PPP.
    - EAP Methods:
      * EAP-MD5
        + Basically MSCHAP. Takes passwords and hashes them into an MD5 hash.
      * EAP-PSK
        + Uses pre-determined symmetric keys.
        + Similar to WPA/WPA-2
      * EAP-TLS
        + EAP handles full blown TLS.
        + Needs a server and client certificate.
      * EAP-TTLS
        + Uses TLS exchange method.
        + Only requires server certificate.
    - 802.1X is a full blown authentication standard that allows connections between client system (supplicant) and the network itself.
      * Also known as EAP over Ethernet or EAP 802.11.
      * Creates some form of connection between supplicant and the authenticator, then runs EAP within that for the authentication itself.
      * RADIUS lives on 802.1X.
    - LEAP was invented by Cisco before 802.11i standards. Cisco's high security wireless standard.
      * EAP with a password within a TLS tunnel. Not used anymore.
      * Supplanted by EAP-FAST.
    - PEAP was Microsoft's standard of EAP before EAP. EAP communication within a TLS tunnel. Not used anymore.
  + The Network Firewall
    - Stateful vs. Stateless
      * A stateless firewall will filter and block stuff no matter the situation. Setting a rule to block a port or IP or any content, with no other context, is a stateless firewall setting. Stored into an ACL.
      * A stateful firewall doesn't have an access control list - it looks at what is going on and then makes a decision on what to do. For an example, a stateful firewall that seems a ping flood coming in would then decide to block pings.
  + Proxy Servers
    - Proxies are often application specific, such as a Web Proxy, and FTP Proxy.
    - A transparent proxy has to be in-line to go out to the internet.
    - Two kinds of Proxy Servers:
      * Forward Proxy Server: Hides the clients.
        + Hey proxy 
          Client 
          Forward Proxy 
          Firewall 
          Internet 
          Server 
        + Dedicated boxes within a network.
        + Provides caching, content filtering, acts as a firewall.
        + A nefarious forward proxy:

Client 
Internet 
Proxy 
Firewall 
Server 

It is easy to figure out who is using this proxy due to the internet connecting to the proxy.

An encrypted tunnel (VPN) from the client to the internet to the proxy will fix this concern.

* + - * Reverse Proxy Server: Hides the servers.
        + Client 
          Internet 
          Reverse Proxy 
          Firewall 
          I got you 
          Proxy 
          Server 
        + High security, handles DoS attacks, can provide load-balancing, caching, handles encryption acceleration (like HTTPS encryption/decryption).
  + Honeypots
    - Nothing more than devices that are designed to emulate a host/network to allow you to let the bad guys in and then track what they're doing.
    - The idea of a honeypot is the emulate services that you'd find on a typical server.
    - Need to sit out on the public internet. Often, people put honeypots within a DMZ.
    - A sophisticated honeypot logs every single keystroke.
    - A network can be emulated by using a honeynet.
      * Honeynets are used often in a virtualized environment.
  + Virtual Private Networks (VPN)
    - Connection Options for VPN:
      * Leased line (T3 line, very expensive)
      * Leveraging the internet itself (VPN)
    - A VPN Tunnel is a connection between two VPN endpoints (client and firewall/server)
    - Remote Access VPN - one computer connecting to a LAN.
    - Site-to-site VPN - Two LANs connecting together.
    - A VPN is slow compared to being within a LAN.
    - Split vs. Full Tunnel
      * A full tunnel is where all requests travel through the VPN.
      * A split tunnel is where traffic going to the LAN goes through the VPN tunnel, but any other traffic routes normally through the network card.
    - VPN Setup Steps:
      * Protocol to set up tunnel.
      * Protocol to handle authentication and encryption.
    - VPN Protocols:
      * Point-to-Point Tunneling Protocol (PPTP)
        + Oldest
        + Uses PPP for tunnel
        + Password only.
        + TCP Port 1723.
      * Layer 2 Tunneling Protocol (L2TP)
        + Cisco proprietary
        + Similar to PPTP
        + L2TP tunnel
        + IPsec Encryption (Fast)
        + UDP ports 500, 4500.
      * IPsec VPN
        + Uses IPsec for tunnel and encryption
        + UDP ports 500, 4500.
        + Great for IPv6.
      * SSL/TLS
        + TCP Port 443
        + Works within web browser, clientless.
        + TUN/TAP (Virtual Network Driver) Tunnel
        + TLS encryption
      * OpenVPN
        + Program with its own unique tunnel.
        + Encryption based on SSL/TLS.
        + TCP 1194, can be changed easily.
  + IPsec
    - Type of IP security that works on a host-to-host basis.
    - A bunch of protocols that work together that come up with an idea of two hosts having a secure connection.
    - Two different modes:
      * Authentication Headers
        + Only provides integrity
        + Runs integrity check, inserts Authentication Header before TCP -> Data -> IP Address.
        + This is an HMAC.
      * Encapsulating Security Payload (ESP)
        + Goes through process of encrypting TCP -> Data -> IP Address.
        + Uses AES, 3DES, etc.
    - When referencing keeping the original IP address, we are referencing Transport Mode.
      * Transport Mode in the real world doesn't work well.
    - Instead, we use Tunnel Mode.
      * Get rid of IP header, add new IP address to the data. (AH)
      * The original IP header is encrypted, then a new IP address is added to the outside of the data. (ESP)
    - In IPsec, we use ISAKMP. Internet Security Agreement Key Management Protocol.
      * Its only job is to create a Security Agreement (SA) between two hosts.
      * Two hosts use a negotiation protocol, ISAKMP, to begin talking.
        + Provides Initial Authentication

Certificates

Key Exchange

Preshared keys

* + - IPsec examples:
      * VPNs
        + Pure IPSec
        + IPsec with L2TP
      * RADIUS/TACACS+
        + No native encryption, so IPsec is used to create a VPN tunnel between hosts.
      * IPsec with IPv6
        + IPsec header information can be placed within an IPv6 header.
        + Not used often.
      * Using IPsec with non-secure protocols
        + Could be used, theoretically, with an insecure connection like telnet. It can be used to encrypt the telnet data.
  + NIDS/NIPS
    - Network Intrusion Detection System
      * Passive
      * Often setup as "Out-of-band" which means out of the main LAN.
    - Network Intrusion Prevention System
      * Often setup as "In-Band", which means all network traffic goes through the device to the internet.
      * Active/inline
        + Block ports/username/IP addresses from router.
      * Detection methods
        + Behavioral/anomaly based
        + Signature based
        + Rule-based
        + Heuristic (signature files, behavior/anomaly, learns over time.)
      * How to set this up?
        + Sensors, like a Network Tap. Has In/Out port, which checks every single packet In/Out.
        + Port mirroring, where a switch can be configured to grab data from particular ports/VLANs.
        + Collectors, which are computers that take data from sensors and storing it into a single database.
        + Correlation Engines, which is a tool that does the behavioral anomalies, rule checks, signature checks, heuristic checks.
  + SIEM
    - Security Information and Event Management (SIEM)
      * Aggregation - Grabbing data from different places and storing it.
        + Time synchronization, event deduplication, normalization, logs.
      * Correlation - Analyzing and reporting the data that is collected.
        + Alerting/triggering.
    - Write Once, Read Many (WORM)
      * WORM drives are dated.
      * Not used, most logs are stored on HDDs.
    - Popular SIEM software:
      * Splunk
      * ArcSight
      * ELK (Elastic Search, Log Stash, Kibana) Open-source/freeware.
  + **Section 7: Beyond the Basic LAN**
    - Wireless Review
      * 802.11 Infrastructure Mode
        + Begins and ends with WAP.
        + WAP is a bridge between an 802.11 network and an Ethernet network.
        + Every WAP has a MAC address.

Configured with a Service Set Identifier (SSID)

SSID is broadcast out, and we associate the MAC address of the WAP with the SSID to create a Basic Service Set Identifier (BSSID).

Client sends request to WAP to join SSID, and once it is accepted the client becomes a part of the Associated List.

If multiple WAPs are connected to the same common Ethernet broadcast domain, they become known as an Extended Service Set Identifier (ESSID)

* + - * Wireless Equivalent Policy (WEP) provides basic authentication and encryption.
        + Uses RC4 streaming protocol, using an initialization vector like all streaming protocols.
        + Shared key concept (64-bit or 128-bit)
        + WEP has initialization vector issues and can be easily hacked to obtain the key.
      * Wireless Protected Access (WPA)
        + The draft 802.11i standard, not full. Predated WPA2.
        + Dumped concept of RC4 and replaces it with AES encryption.
        + WEP was replaced with Temporal Key Integrity Protocol (TKIP)

Still uses RC4 but fixes the Initialization Vector issue.

* + - * 802.11i became known as WPA2, once the industry caught up.
    - Living in Open Networks
      * Cookies, like session cookies, with authentication information within it can be exploited.
        + Even though the HTTPS website will secure data, the cookie itself causes a security vulnerability.
        + The cookies itself are not sent over a secure connection.
        + Replay attacks (SSL stripping) can be used when cookies are sniffed.
      * How do we protect our assets?
        + Use secure protocols on unsecure networks.
        + Use HTTPS on websites that collect information.

HTTP Strict Transport Security (HSTS) requires users to constantly use HTTPs.

* + - * + Use VPN in non-secure networks.
    - Vulnerabilities with Wireless Access Points
      * A Rogue AP is nothing more than an unauthorized access point.
      * An Evil Twin is a Rogue AP with the same intentional SSID the same of a private.
      * 802.11 jammers are illegal in the US. They can create denial of service attacks, or jam wireless channels that makes clients jump to the Evil Twin. This is now a Man in the Middle attack.
      * In the absence of an 802.11 jammer, someone can use a De-Authentication Attack.
        + Running a program to show all clients on a particular SSID, and then sending deauth commands to kick everyone off the network. Then, have all clients connect to the Evil Twin.
    - Cracking 802.11 - WEP
      * WEP is the oldest 802.11 standard.
      * The initialization vector generation is susceptible to IV attacks within WEP.
      * Aircrack can be used to crack WEP keys.
      * Kali Linux listening on WLAN NIC using Airodump, selecting the target SSID, listening on that SSID and then using the dumpfile to crack the key for it.
      * Can mathematically be cracked by looking at packets.
    - Cracking 802.11 - WPA
      * WPA is using RC4 but TKIP with it. WPA2 is using AES with CCMP.
      * The initial connection between a device and WAP using WPA/WPA2 uses a 4-way handshake.
        + This is the most vulnerable aspect of WPA/WPA2.
      * WPA/WPA2 crackers require a dictionary file in order to be cracked.
      * Once the handshakes are captured and put into a dumpfile while being monitored, the network can attempted to be cracked using a dictionary file.
      * Use long, complex private shared keys when using WPA/WPA2.
    - Cracking 802.11 - WPS
      * WiFi Protected Setup (WPS) which is push-button configuration.
      * WPS Weaknesses:
        + 8 digit key for WPS is actually 7

2 to the 7th power.

One of the eight digits is just redundancy check for the other seven.

* + - * + Key exchange is first processed in 4-bits then 3-bits.
        + That means only 11,000 iterations are needed to crack it.
        + WPS capable access points can detect an attack and shut down or turn off WPS.
      * Prevention:
        + Get rid of older routers.
        + Firmware updates.
        + Consider a modern wireless router.
    - Wireless Hardening
      * Survey/Installation Issues
        + Survey tools

Site survey programs find SSIDs, MAC addresses, bands/channels/signals.

Documents all of the above information.

Often has a heatmap, which shows the signal strength of all access points within an environment.

* + - * Maintaining existing wireless networks/Monitoring wireless networks
        + Good wireless documentation.

Take advantage of survey tools and continue to keep it documented.

* + - * + AP isolation enabling

All wireless devices on that SSID can see the access point and get to the network, but they cannot see each other.

* + - * + Implement 802.1X for encryption and crackability.
        + Scan the network. A wireless intrusion detection system will accomplish this constantly.

A WIDS can be software or physical systems.

Monitors wireless radios.

Watches for rogue access points.

Knows MAC addresses of authorized equipment

Watches working protocols

* + - * Defend wireless clients
        + Hardening wireless clients include training users to detect rogue access points/evil twins by simply looking at SSID lists.
    - Wireless Access Points
      * Thick (Fat) client - Standalone wireless access point.
        + Device that has to be configured by itself.
      * Thin client - Centrally managed and configured. Controller-based.
      * Many wireless access points have the ability to have an external antenna plugged into it.
        + Antennas have their strength measured in Decibels, or DBI.
      * Antenna Types:
        + Omni/Omni-Directional

Signal goes every direction.

* + - * + Dipole

Meant to be used on a single level or floor.

Has little adjustments.

Extremely common.

* + - * + Directionals

Long beam signal.

Yagi - Designed to pick up and send a pointed signal.

Parabolics - Radar dishes, more powerful than a Yagi.

* + - * + Patch

Half of an omni.

Half of a sphere. Sends signal in one direction 180 degrees, none behind it.

* + - * Antenna Placement:
        + Big basketball stadium, use an Omni.
        + Outdoors, use a Dipole.
        + Against wall, use a Patch.
        + Long distances between buildings, use a Directional.
      * Band Selections:
        + 2.4GHz or 5GHz bands.
        + How to choose? Determine the following: Technology used, speed wanted, and how crowded the area is.
        + With a 5GHz band, channel width is an issue.

Generally, the wider the channel, the better the throughput.

The channel width being wider makes it harder to hop channels as the options become limited.

* + - * + Automated channel selection is common.
    - Virtualization Basics
      * Virtualization simply means to virtualize everything about a computer into a virtual system.
      * The idea behind virtualization:
        + Host system with real hardware, virtualizing it.
        + A virtual computer takes advantage of the real hardware by using it.
      * Emulation uses software to imitate hardware.
      * Virtualization provides power saving, space saving (multiple virtual servers on one physical device), better system recovery, better duplication, research.
      * Hypervisor - Virtual Machine Monitor (VMM)
        + Hypervisor, type 2 - Runs on top of Host OS.
        + Hypervisor, type 1 - Runs directly on top of hardware, independent of host OS.
    - Virtual Security
      * Virtualization by itself is a security feature.
        + Patch management
        + Centralized hardware maintenance
        + Resilient and high availability
        + Great testing and sandboxing environment
        + Network separation

Virtual switching allows this to happen.

VLANs

* + - * + Snapshots and backups
      * Virtual threats
        + Anything that can happen to a physical machine, can happen to a virtual machine.
        + Malware
        + Bad patch management
        + Policy management
      * Cloud-based infrastructure providers will provide their own security-as-a-service (SaaS)
      * VM sprawl is where, within one network, multiple types of hypervisors and VMs are deployed with multiple means.
      * VM escape is where a hacker is able to "get out" of the VM itself and cause damage to the hypervisor.
      * Virtualization Hardening
        + Remove remnant data
        + Make good policies
        + Define user privileges

Within the hypervisor itself, who can create/edit/delete VMs?

* + - * + Patch everything
        + Cloud Access Security Brokers (CASB)

A CASB acts as an intermediary between your infrastructure and the cloud.

Typically a cloud-based service.

Makes sure policies are controlled, watches for malware.

* + - Containers
      * A container is an application and all of its libraries and binaries running on top of a kernel.
      * A container runs isolated instances of programs and services.
      * Containers are self-contained applications that can communicate with network resources that have been explicitly allowed.
      * Whatever is inside a container can only see what is inside its container. No access to any underlying operating system's files or folders, cannot see any networking information, etc.
      * The container stays isolated, therefore there is less attack surface. If a container is compromised, they would not have access to anything else but what is inside the container.
    - IaaS
      * Infrastructure-as-a-Service
        + An entity sets up a virtual infrastructure to sell to an administrator.
        + Physical equipment hosted by another company.
        + Examples:

Microsoft Azure

Amazon Web Services

* + - * + Ability to create an infrastructure of an entire network, server setup, public IP address, firewall/security policies, etc. all at the click of a button.
    - PaaS
      * Platform-as-a-Service
        + Usually has some IaaS aspect within it.
        + Typically meant for developers to create and deploy applications.
        + Examples:

Heroku

Google App Engine

OpenShift

* + - * + Program/code that is written will be uploaded within the PaaS, check the code, bring libraries, etc. and then create a URL to be deployed.
    - SaaS
      * Software-as-a-Service
        + Predates virtualization.
        + A subscription-based license.
        + Gets rid of optical media
        + Examples:

Microsoft 365/Office 365

Google Apps

DocuSign

* + - Deployment Models
      * Referencing deploying applications once created.
      * Examples:
        + On-Premise Deployment

Using physical servers in an environment to continue to scale with the application's scale.

* + - * + Hosted Application

Using resources from another company to host the application.

This turned into cloud-based hosting, through virtualization.

* + - * Types of Clouds:
        + Private Cloud

Virtual machines built within an organization, for that organization. It is private.

* + - * + Public Cloud

Open-for-business virtual machines, like Microsoft Azure or Amazon AWS.

* + - * + Hybrid Cloud

Partially segregated as private, with some as public to be resold.

* + - * + Community Cloud

Differing organizations putting in money to build one cloud shared amongst those organizations.

* + - * Virtual Desktop Environment (VDE)
        + Local client that is controlling a remote system.
        + RDP within Windows, for example, is a type of VDE.
        + The local client essentially becomes a terminal to send commands to the target machine.
      * Virtual Desktop Integration (VDI)
        + Complete operating systems that are deployed in a cloud environment to be accessed by a terminal client.
        + Accessing a virtualized environment within the cloud.
    - Static Hosts
      * Refers to devices that have embedded OS and some type of network awareness, from a Google Home to a Nest Thermostat, to a game controller, etc.
      * A static host is typically referred to as a device designed for a specific (single) purpose.
      * Also referred to as an Internet-of-Things (IoT) device.
      * Industrial Control Systems (ICS) is a general term that encompasses control systems for process control, like an HVAC unit that has a specialized single-purpose.
      * Supervisory Control and Data Acquisition Systems (SCADA) are just like ICS but typically have a cellular WAN connection and have autonomy to accomplish their tasks.
      * Securing Static Hosts
        + Change default passwords
        + Turn off unnecessary services
        + Monitor security and firmware updates
        + Defense-in-depth, or creating layers of protection around that device.
        + Network segmentation
        + Treat a static host like any regular host.
    - Mobile Connectivity
      * SATCOM
        + Satellite Communication
      * Bluetooth
      * Near-field Communication (NFC)
        + Very short range wireless connectivity, similar to Bluetooth.
        + Physical contact/near-physical contact needed.
        + When it's turned on, no security.
      * ANT/ANT+
        + Simple form of wireless communication.
        + Slow, but well-protected.
      * Infrared
        + Often times, Android phones have Infrared transmitters. Not receivers
      * USB
        + USB On-The-Go (OTG) is a two-way USB type that can be ingoing or outgoing, which isn't part of the USB standard itself.
        + This is a security vulnerability.
      * Wi-Fi Direct/Tethering
        + 802.11 Ad Hoc mode - Rare connection type, where two devices (such as smartphones) connecting to one another.

Wi-Fi Direct is used on many streaming devices today, such as Roku. It uses WPS, which is a security vulnerability.

* + - * + Tethering - Linking a computer to a smartphone or vice versa in a wired connection, to leverage the resources of either or.
        + Wireless Tethering - A mobile hotspot, that needs to be secure.
    - Deploying Mobile Devices
      * Mobile Device Management Tools - A central management device for mobile devices linked to that software.
      * Mobile Application Management - Containerized management scoped to only the applications on the mobile device.
      * Corporate vs. Personal Use
        + Corporate Owned, Business Only (COBO)

Company Owned

Company decides what to do, such as:

Encryption

Applications

Wireless types

* + - * + Corporate Owned, Personally Enabled (COPE)

Everyone has the same device.

Devices are controlled by company

People will still want to use their own devices

Learning curve

* + - * + Choose Your Own Device (CYOD)

Users select from approved devices

Less of a learning curve

* + - * + Bring Your Own Device (BYOD)

Users choose based on their experiences.

Learning curve decreased

Heavy device/application management

* + - Mobile Enforcement
      * Sideloading
        + Process of getting around an application store (Google Play, Apple Store) to upload product to consumers.
        + Often times, developers use this to test products.
        + Extremely difficult to do on Apple platform, easy on Android.

Android devices can have this limited through mobile management.

* + - * Carrier Unlocking
        + In the US, companies are required by law to allow phones to be unlocked.
        + Small security issue is really only when the device is being managed, and the user unlocks that phone from the carrier.
      * Rooting/Jailbreaking
        + You do not have root access when you purchase a phone.

This makes it harder for users to reformat firmware, install malware, or abuse the system.

The manufacturer retains root access.

* + - * + Issues with rooting:

Auto updates are disabled.

Trouble access the store, such as Google Play.

Exposure to malware

* + - * "Big Brother" monitor points when managing mobile devices:
        + Firmware OTA updates
        + Camera Use
        + SMS/MMS (Texting)
        + External media
        + Microphone/GPS tagging
        + Payment methods
    - Mobile Device Management
      * Content Management
        + Applications management
        + Databases
        + Documents
        + Geolocation
        + Geofencing

Geolocation with a geographic trigger to take action

* + - * + Push notification services

Applications will push notifications if you want

* + - * + Passwords/PINs

Set requirement of use.

Can recover passwords.

* + - * + Biometrics

Fingerprints

Facial recognition

Vocal recognition

Can be used to configure applications, lock/unlock devices

* + - * + Screen locks
        + Remote wipe
      * Application Management (MAM)
        + Versioning
        + Updates
        + Patches
        + Specific to application
        + Context-aware authentication

Where is the user?

What time of day are they trying to authenticate?

What OS is being used?

* + - * + Storage Segmentation

Dedicated a storage space of the mobile device for our applications

* + - * + Full device encryption

Encrypting entire storage of the device.

* + - * + Containerization

One container for an application or group of applications to keep them separate

* + - Physical Controls
      * Deterrent Physical Controls
        + Designed to prevent malicious access to physical infrastructure.
        + Outside lighting
        + Signage
        + Security guards
      * Preventative Controls
        + Fences
        + Barricades

K-Ratings - Super strong fences meant to stop vehicles.

K4 - 30mph

K8 - 40mph

K12 - 50mph

* + - * + Mantrap

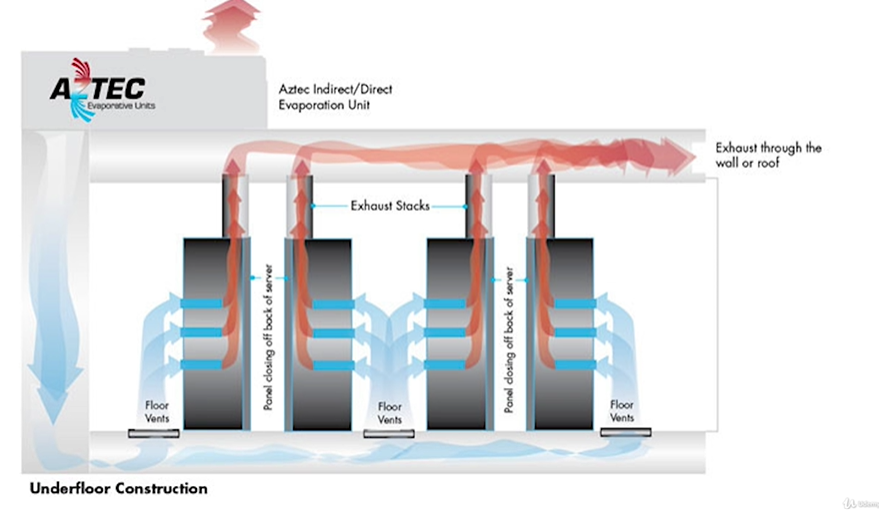
Entry system that consists of two-doors.

* + - * + Airgap

Separating important cabling infrastructure from everything else.

* + - * + Safe
        + Locked cabinets/enclosures
        + Faraday Cages

Meant to block EMI/radio frequency to protect sensitive electronic equipment.

* + - * + Locks/Key Management
        + Cable locks
        + Screen filters
      * Detective Tools
        + Detects malicious intent being carried out.
        + Alarms
        + Cameras
        + Infrared detectors
        + Log files
      * Compensating and Corrective Controls
        + Example: Extra security guards in the middle of a breach.
        + Not as detailed or important for physical controls.
    - HVAC
      * The cooler a piece of electronic is, the better it runs.
      * Infrared Cameras (Thermal Imagers) are important within HVAC systems, to detect hot zones and leaks.
      * Zone-based HVAC is used in office environments in which specific areas have their own thermostat.
      * Hot and Cold Aisles
        + Server 
          Cabinets 
          (Side view) 
          CRAC 
          Seal Barrier 
          for pressure balance 
          Server 
          Cabinets 
          (Side view) 
          Hot Aisle 
      * Contained System
        + 
      * Securing HVAC
        + Leave an air gap - keep the HVAC system separated from the network.

Use VLAN for isolation, if an air gap cannot be used.

MAC filtering can be used here.

* + - * + Remote monitoring - This can be a security concern. Work with vendors/suppliers for SLA, to make sure VPNs are being used.
    - Fire Suppression
      * Fire Extinguisher Classes
        + Class A: Designed for ordinary solid combustibles, like wood.
        + Class B: Designed for flammable liquids and gases.
        + Class C: Designed for energized electrical equipment.
        + Class D: Designed for combustible metals.
        + Class K: Designed for oils and fats.
      * Do not use water to put out an electrical fire.
      * FM-200 is the golden standard today for server room fire suppression.
      * Seal off the server room.
  + **Section 8: Secure Protocols**
    - Secure Applications and Protocols
      * SSH Protocol
        + Secure Shell. Port 22.
        + Always has the server pass the key for a key exchange for encryption.
        + SSH applications have built-in encryption.
      * HTTP protocol
        + The webpage itself is not encrypted.
        + TLS acts as an intermediary between the web page and web browser to perform the encryption.
        + TLS was invented for websites, but can work with multiple other applications.
      * Anything on the internet will either be an application with encryption built-in, or taking advantage of protocols.
    - Network Models
      * OSI Seven-Layer Model
        + 7 - Application
        + 6 - Presentation
        + 5 - Session
        + 4 - Transport
        + 3 - Network
        + 2 - Data Link
        + 1 - Physical
      * TCP/IP Model
        + 4 - Application
        + 3 - Transport
        + 2 - Internet
        + 1 - Network Interface
    - Know Your Protocols - TCP/IP
      * IP addressing
        + IPv4

Four octets separated by three dots, each octet is a binary value of 8. This makes a 32-bit address.

Private vs. Public IP addressing

An ISP will assign a public IP address for internet access for a network, and all the devices within the internal network will have private IP addresses.

A private LAN will have a router separated from the internet using Network Address Translation (NAT).

Private Ranges:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 173.31.255.255

192.168.0.0 - 192.168.255.255

* + - * + IPv6

Up to 128-bits.

A device will have two IPv6 addresses:

Link Local - FE80

Generated automatically by individual hosts.

Internet address

* + - * Transport Protocols:
        + TCP

Does most of the work on the internet.

Connection-oriented protocol

A client sends a "Hello" to the server, the server will "ACK", and then the client sends its data.

This is a three-way-handshake.

* + - * + UDP

Connectionless

No acknowledgment

Sends lots of packets

Used with a high degree of confidence that the target is listening.

* + - * + ICMP

Main job is to handle ARP, Pings, and small things.

One packet.

* + - Know Your Protocols - Applications
      * Hypertext Transfer Protocol (HTTP)
        + Port 80
      * Secure Hypertext Transfer Protocol (HTTPS)
        + Port 443
      * Telnet
        + Port 23
      * Secure Shell (SSH)
        + Port 22
      * File Transfer Protocol (FTP)
        + Port 20 and 21
      * FTP/SSH
        + Port 22
      * FTPS
        + FTP with SSL/TLS security.
        + Port 20 and 21
      * Secure File Transfer Protocol (SFTP)
        + Port 22
      * Secure Copy (SCP)
        + Port 22
      * Trivial File Transfer Protocol (TFTP)
        + Port 69
      * NETBIOs
        + Port 137, 138, 139
      * Server Message Block (SMB)
        + Port 445
      * Simple Mail Transfer Protocol (SMTP)
        + Port 25
      * IMAP
        + Port 143
      * POP
        + Port 110
      * Domain Name System (DNS)
        + Port 53
      * DHCP
        + UDP Port 67/68
      * Simple Network Management Protocol (SNMP)
        + Port 161/162
      * LDAP
        + Port 389
      * Remote Desktop Protocol (RDP)
        + Port 3389
    - Transport Layer Security (TLS)
      * Originally invented for websites, but it is used all over the internet.
      * Secure Sockets Layer (SSL)
        + Series of security protocols
        + Been around for a long time
        + Usurped by TLS
      * TLS is newer than SSL, but accomplishes the same things.
        + TLS is more secure than SSL.
    - Secure Connection (SSL/TLS key points):
      * Encryption
        + A symmetric encryption, which is faster than asymmetric.
      * Key exchange
      * Authentication (SSL/TLS uses RSA certificates)
      * HMAC (Hashing)
    - Internet Service Hardening
      * Using secure protocols are always preferable to insecure protocols.
      * DNS (Domain Name Services)
        + Runs on port 53.
        + Nonsecure protocol.
      * DNSSEC
        + In the 90s, DNSSEC was forwarded as a tool to make DNS servers have some form of security/authentication.
        + DNS server generates a key pair and the upstream DNS server signs them, creating new DNS records for each zone.
        + One key is a Public Signing Key.
        + Not an encryption, it is purely an authentication tool.
        + Popular for public DNS servers, like Google's 8.8.8.8.
      * Email
        + SMTP/POP/IMAP have always been insecure, but secure versions of them all have become more secure.
        + SMTP

Secure SMTP creates a TLS connection between the client and server, so the data is sent with authentication and encryption.

SMTP uses 25. Secure SMTP does 465 or 587.

* + - * + IMAP/POP

Now, StartTLS is used. It is an extension to IMAP/POP.

An encrypted TLS tunnel is created.

IMAP uses port 143, SSL/TLS IMAP uses 993.

POP uses 110, but SSL/TLS POP uses 995.

* + - Protecting your servers
      * SSL Accelerator
        + If a lot of asymmetric encryption is used, SSL/TLS will be used a lot. This is a burden for CPUs.
        + A special card can be installed into each server, and their only job is to encrypt/decrypt asymmetric encryption on the fly.

Or, a special SSL Accelerator device can be installed behind the router facing the servers that serves the same purpose.

This is better for environments with large amounts of servers.

* + - * Load Balancer
        + Actually like a proxy, as it takes all incoming requests from the router and sends them to the servers.

This can be determined by workload, DNS names, IP, etc.

* + - * DDoS Mitigator
        + A device placed between the router and servers.
        + Detects when DDoS attacks come through.
        + Reaches out to a third party like CloudFlare upon detection, which then those CloudFlare servers on the internet acts as a proxy to filter out the bad data.
    - Secure Code Development
      * Waterfall Model (Old fashioned and rigid model)
        + Requirements
        + Design
        + Implementation
        + Verification
        + Maintenance
      * Agile Model (New and common model today)
        + Kickoff 
          Sprint 
          Planning 
          Test 
          Demo 
          Deployment 
          Agile Model 
          Sprint 
          Planning 
          Test 
          Demo 
          Deployment 
          Sprint 
          Planning 
          Test 
          Demo 
          Deployment 
        + Toolsets within the Agile Philosophy

Sprint: A short time period of deadline where whatever can be achieved, is.

Scrum: A short meeting about work done, roadblocks, next tasks.

* + - * DevOps
        + Methodologies and tools allowed for development and operations to get a product out of the door.
        + DEV 
          OPS 
        + Just because a product is delivered doesn't mean that the development on it has ceased.
      * Secure DevOps
        + Run security automation tools.

Fuzzer tools, static testers, Intrusion Detection

Always look for vulnerabilities in code.

* + - * + Change management/version control

Change will happen.

Organization, authorization, documentation

Continuous integration

* + - * + Baselining

Baselining critical security objectives

Encryption

Input validation

Any baseline set forth

* + - * + Consider immutable systems

An immutable system has interchangeable parts

Embedded firmware device

Virtual machine

* + - * + Infrastructure as code

Create preset definition files

* + - Secure Deployment Concepts
      * Compiled vs. Runtime Code
        + Most applications ran today are Runtime Applications.
        + Runtime code is not compiled; it is not executable. It is read by whatever you are running, like a web browser, and shown to you.
        + Compiled code is executable code.
      * Proper error handling
        + Any application generates errors.
        + The application should recognize errors and put up a screen saying "Oops!" or similar.
      * Proper input validation
        + Validating an input in a type box to display to the user that it does not meet the requirements somehow.
      * Normalization
        + Avoid replication of data.
        + Tools like indexing are used for databases that are normalized.
      * Stored Procedures
        + Stored Procedure 
          Zip Code Table 
          ZipcodO Zip 
          Nome Table 
          LastName FirstName Address 
          Birthday Table 
          1001 
          1002 
          77088 
          71433 
          Queru 
          Smith 
          Jones 
          1001 
          1002 
          Smith 
          Jones 
          John 
          Ted 
          1070 
          2174 
          1001 
          1002 
          7/6/66 
          9/10/72 
          •p code = 770 
          Stored Procedure 
          heck input 
          validatio 
          Database 
      * Encryption/Code Signing
        + Digitally signing code to ensure it is good order.
      * Obfuscation (Camouflaged)
        + Not a full blown encryption of code, but the desire is to keep it from being copied.
        + A minifier tool can be used to remove all spaces and excess carriage returns to leave just the code itself.
      * Code reuse/Dead code
        + If known-good code can be reused, do it.
        + Dead code is also referred to code that is no longer being used. A good rule of good code is to cut it out; it can be taken advantage of.
      * Server-side vs. Client-side Execution/Validation
        + Client-side execution puts a lot of code and security on the client.

Security is only as good as the client's security.

* + - * + Server-side execution puts a lot of work and load on the server.
      * Memory Management
        + All applications use memory.
        + The process of memory management is involved and requires testing.
      * Third-Party Libraries
        + Security issues can arise from these.
        + A backdoor can be found in a weakness within a third-party library to exploit the application.
      * Data exposure
        + If data is a part of your application, that data is always at risk of exposure.
        + Today, we always go through aggressive encryptions client-side and server-side to protect data that is exposed.
    - Code Quality and Testing
      * Static Code Analyzers
        + Look at actual code for standard types of errors that happen often.
        + Not running code, just reading it.
      * Dynamic Analysis
        + Runs the code.
        + Looks for logic errors, security holes, memory leaks, fuzzing ability.
      * Staging
        + Staging is the point where more realistic environments are created to see how the code holds up.
        + Stress Test

Putting the code under load to check for security/stability vulnerabilities.

Often times in a sandbox environment.

* + - * + Model Verification

Verifying the "model" - is this code doing what we envisioned it to do at the beginning?

* + - * Production
        + Taking code off the sandbox, putting it onto production servers.
  + **Section 9: Testing Your Infrastructure**
    - Vulnerability Scanning Tools
      * Tracert
        + Used to gather network information as part of an assessment.
      * Advanced IP Scanner
        + Freeware tool used to scan an internal network for NIC types, MAC addresses, IP addresses, shared folders.
      * Nmap
        + A powerful network discovery tool.
        + Finds clients on a LAN and discovers open ports.
      * Microsoft Baseline Security Analyzer
        + Uses the Microsoft Knowledge Base to check for patches, security vulnerabilities, Windows firewall status on an individual system.
      * To check entire infrastructures, Vulnerability Assessment tools are needed.
        + Nessus
        + Nexpos
        + OpenVAS
    - Vulnerability Scanning Assessment
      * Vulnerability assessments require authorization from management.
      * Credentialed vs. Non-Credentialed
        + A credentialed VA means you have the usernames and passwords, from an insider perspective.
        + Non-credentialed is not having any usernames and passwords, from an outsider perspective.
      * Intrusive vs. Non-Intrusive
        + Intrusive is trying to exploit and actually perform an action to corrupt something, whereas non-intrusive is just scanning and assessing.
      * Misconfigurations
        + Often times, a misconfiguration (like a default username/password) can present a vulnerability.
      * False positives
        + When an assessment flags a problem, but in reality it isn't a problem.
      * Compliance
        + PCIDSS, for example, monitor credit card usage.

These compliance rules have to be applied to items that handle credit card data.

* + - * Remember to get authorized!
    - Social Engineering Principles
      * Social engineering is simply people tricking people.
      * Social engineering principles:
        + Authority

To impersonate or imply a position of authority

* + - * + Intimidation

To frighten by threat

* + - * + Consensus

To convince of a general group agreement

* + - * + Scarcity

To describe a lack of something

* + - * + Familiarity

To imply a closer relationship

* + - * + Trust

To assure reliance on their honesty and integrity

* + - * + Urgency

To call for immediate action

* + - Social Engineering Attacks
      * Types of attacks:
        + Physical Attacks

Tailgating

Waiting for someone with access to a building/door and following them.

Shoulder surfing

Dumpster diving

* + - * + Virtual Attacks

Phishing

E-mails

Spear Phishing

Directed towards specific person or organization.

Whaling

Spear phishing directed towards executives

Vishing

Uses telephone system to steal private information.

Hoax

Warns someone that something bad is happening when it's not.

Watering hole attack

An attempt to infect websites that a group of end users frequent to gain access to their information or network.

* + - Attacking Web Sites
      * In order to recognize an attack, you need to be able to read log files.
      * Common Log Format (CLF)
        + All web servers generate logs in the same format.
        + - [10/Oct/201710℃5 거 -0600] "GET /CompTIA09-srndll 
          12700.1 - 
          HTTP/1 0" 200 다2기3 
        + This log has, in order from left to right:

Host IP address: 127.0.0.1

Ident (Identity Check): - -

Authuser

Date/time

Request (within quotes)

Also known as the data payload.

Status (three digit HTTP status code): 200

Bytes (excludes HTTP headers): 42213

* + - * Some websites have a central control panel, like cPanel, that monitor connections to it that it views as malicious.
        + Here is an example of an email that cPanel can send to the administrator:
        + PID: 3948 (Parent PID: 2934) 
          Account: Admin25 
          Uptime: 62 seconds 
          Executable: 
          /usr/local/bin/php 
          Command Line (often faked in exploits): 
          /usr/locol/bin/php/home/totdlcentrol/public_html/qenerotor/runcrowl php 
          Nework connections by the process (if ongl 
      * Web site attack types:
        + Cross-site scripting

Also known as XSS.

Client-side script injected into trusted web sites.

* + - * + XML injections

Inserts XML information that shouldn't be there altering the logic of the program.

* + - Attacking Applications
      * Typically there are web-based applications, or local applications.
      * Types of attacks:
        + Injection Attacks

Adding extra information into an input/application that causes malicious intent.

Code injections: adding extra code to manipulate the program.

Command injections: using the application to get to the underlying OS.

SQL (Structured Query Language) Injection

Using SQL commands to access SQL database.

SQL query terms:

Inner join

Select from

Insert into

LDAP Injections

LDAP is based on X.500 and uses TLS encryption.

Poorly formed applications can be taken advantage of by putting LDAP information into them and creating LDAP injections.

* + - * + Buffer Overflow

Anytime data is entered into an application, it enters a buffer.

A buffer is a reserved part of memory to store data before it is input into the application itself.

Locking a system up by repeating the same action so much that the buffer crashes.

* + - * + Integer Overflow

Any variable within an application usually is declared at the beginning of the program itself.

Generating errors based on exploiting a fixed value limit, such as multiplying a number on a calculator to be too large to calculate.

* + - Exploiting a Target
      * A vulnerability assessment is from an insider perspective, never trying to grab any data. A penetration test is from an outsider perspective in which data is obtained.
      * Pen Test Steps:
        + • Get authorization 
          • Define targets 
          • Attack model 
          • Discover vulnerabilities 
          • Reconnaissance 
          • Tru to get information 
          • Exploit vulnerabilities 
          • Grab user nomes and passwords 
          • Toke ddtd from d database 
          • Corrupt webpage 
        + An attack model defines what an attacker knows before starting the penetration test.

White box:

Attackers have extensive knowledge of the target.

Attackers are more like trusted insiders.

Cheapest and fastest.

Black box:

Attackers know nothing about the target.

Attackers are more like stranger outsiders.

External hacking.

Potentially expensive and slow.

Gray box

Somewhere between the two.

* + - * + Reconnaissance

Passive discovery

Not putting any packets on the target; just making phone calls, just doing WHOIS lookups.

Semi-passive discovery

Putting packets onto the target, but nothing that will raise alarms.

Active discovery

Putting packets onto the target, running scanners, running actions that could potentially flag alarms.

* + - * + Exploiting the target

Banner grabbing

Pivot: Uses compromised system to attack other systems.

Persistence: To connect again easily with your target with open timelines.

Privilege Escalation: Ability to gain access to data and resources.

Metasploit, for example, is a framework tool that uses banner grabs to gain information on a system and make listings of the known vulnerabilities with that system from databases.

The tool can then be used to scan and inject systems.

* + - Vulnerability Impact
      * Embedded System
        + An immutable system that never changes. They are easily forgotten and can often be behind on patches.
      * Lack of vendor support
        + Big issue with primarily hardware.
        + Typically happens when the vendor tries to move on, or if the vendor company no longer exists.
        + The issue is the device/system will not have any patches/new parts.
      * Misconfiguration
        + A default configuration is a misconfiguration and massive vulnerability.
        + There are massive databases of default credentials that can be leveraged.
        + Could also refer to a misstep, such as turning on/off a service that needs to be off/on and is now vulnerable.
      * Improperly configured account
        + A user/system account with the incorrect permissions, for example.
        + It is not just permissions, it is also rights.
        + Potential for too much privilege or too little.
      * Vulnerable business processes
        + Unconsidered business processes that cause vulnerabilities.
        + An example is onboarding/offboarding processes of employees/clients, or incorrect storage of sensitive information.
      * Memory/buffer vulnerabilities
        + Resource exhaustion, memory leak, DLL injection, buffer/integer overflow, pointer dereference.

Running out of memory: Resource exhaustion or memory leak.

Either get more RAM or stop the process doing this.

Overflows: Buffer or integer overflows will cause systems to behave unintentionally.

Backdoors: Pointer dereference/DLL injection.

* + - * System sprawl/Undocumented assets
        + A system/device being undocumented or unknown means it is not being controlled and/or protected as an asset, which means it is vulnerable due to lack of administration.
  + **Section 10: Dealing with Incidents**
    - Incident Response
      * The CompTIA Security+ is heavily based on the *NIST 800-61 Computer Security Incident Handling Guide*.
      * Incident Response Process:
        + Preparation

The big plan.

Who is doing what?

Organize the types of incidents that might happen.

* + - * + Reporting

What reports go to whom?

Escalation

* + - * + Practice Scenarios
        + Identification

Recognize what incident has occurred.

Check monitoring tools, alerts, logs.

Expect reports from users.

Assess the impact.

Define who is involved.

* + - * + Containment

Mitigate the damage

Stop the attack

Segregate the network, shutdown the system, turn off a service.

* + - * + Eradication

Remove the malware, close off the vulnerability.

Add new controls.

* + - * + Recovery

Restore from backups, pull snapshots

Hire replacement personnel

Monitor to ensure good operations

* + - * + Documentation

What failed?

What worked?

Generate final report.

* + - * Incident Response Plan
        + Cyber Incident Response Team (CIRT)

A group of people whose job is to respond to all cyber incidents.

Consists of an IT Security Team

Includes IT department and HR.

Legal matters may be included, as well as PR.

* + - * + Document incident types/category definitions

Physical access

Malware

Phishing

Data access

Social engineering

* + - * + Roles and responsibilities

Users: How do they report an issue?

Help desk

Human Resources

Database manager

Incident hotline: A hotline used to report incidents.

IR Manager/Officer

IR Team

* + - * + Reporting requirements/escalation

Determine severity/level

Have a clear chain of escalation.

Informing law enforcement

* + - * + Practice

Annual scenario drills.

* + - Digital Forensics
      * Typically forensics occurs within IT Security for the following reasons:
        + Incident occurs
        + Legal hold
      * Chain of Custody
        + Gathering evidence
        + Presenting evidence with data of high integrity
        + Chain of Custody Form:

Property Record Number: 
Anywhere Police Department 
EVIDENCE CHAIN OF CUSTODY TRACKING FORM 
Case Number: 
Submitting Officer: (Name/lD#) 
Victim: 
Suspect: 
Date/Time Seized: 
Offense: 
Location of Seizure: 
Item 
Quantity 
Descri n of Evidence 
Description of Item (Model. Serial Condition. Marks, Scratches) 
Chain of Cust 

Define the evidence

Document collection method

Date/time collected

Person(s) handling the evidence, with contact information.

Function of person handling evidence

All locations of the evidence

* + - * Order of volatility
        + Memory

Process/services, caches, routing tables, ARP tables

* + - * + Data on the disc

Applies to optical/flash drives

Cache files, temp files, swap files

Write blocker enabled tools

* + - * + Remotely logged data

Web site data

Remote file server logs

* + - * + Backups

Identifying trends

Low volatility takes time to gather data

* + - * Checklist for digital forensic data acquisition:
        + Capture the system image

Write-blocking tools are preferred here.

* + - * + Network traffic and logs
        + Capture video

Taking video of physical surroundings of system.

Capture files of video/audio on system.

Security cameras nearby.

Record time offset.

* + - * + Take hashes

Hash every file and image.

Most forensic tools use built-in hashing.

* + - * + Take screenshots
        + Interview witnesses
        + Track man hours
    - Contingency Planning
      * Disaster Recovery
        + How do we recover from a specific disaster?
        + Evacuation plan

Backup site

Cold site

Takes weeks to bring online. Basic office space.

Warm site

Takes days to bring online. Has some operational equipment, but little to no data.

Hot site

Takes hours to bring online. Real-time synchronization.

Almost all data ready to go. Often a quick update.

Distance and location should be considered for a backup site.

Internet requirements need to be considered.

Housing and entertainment for employees.

Legal issues

* + - * Business Continuity
        + How do we keep our business churning?
        + Order of Restoration

Check power. All outlets, checking AC power.

Check wired LAN.

ISP link

Active Directory/DNS/DHCP servers

Accounting servers

Sales and accounting workstations

Production servers

Production workstations

Wireless

Peripherals (Printers, cameras, scanners)

* + - * Annual exercises
        + Can be tabletop exercises, or physical drills.
        + Failover tests
      * Alternative processing sites
        + Larger organizations may have different processing sites for specific departments. Sharing spaces.
      * Alternative business practices
        + How do we take credit card information?
        + Sales taxes for being in a different state in a disaster.
      * After action reports
        + Clear and detailed documentation of everything that happened for future preparation.
    - Backups
      * Backup methods:
        + External HDDs, tapes, clouds.
        + Full backup: Backup everything.
        + File systems have features to know when files have been changed.

Differential backup: Backup all of the changes since the last full backup.

Less backup sets, but a larger size.

Incremental backup: Only backs up changes made from last backup of any type.

More backup sets, but a smaller size.

* + - * + Snapshots

Typically under virtual machines.

Making a copy of something that happened in the past.

Typically not stored on separate media.

* + - * Backup media:
        + Local

Tapes, NAS, hard drives, etc.

* + - * + Offsite

Backed up in a different location

* + - * + Cloud backups

Take larger time to get full backup, however once it is made, most do a continuous incremental backup.