CompTIA Security+ Notes Part 1

Non-repudiation (ensuring undeniable proof of participation in actions)
- Immediately think to digital signatures

Digital signature - hash and encryption
- Serves as undeniable truth
- Hash and encryption

Confirms authenticity
- No assurance of email without digital signature to verify who sent it

Ensuring Integrity
- Any alterations provides proof through hashing

Accountability
- People know their actions can be traced back
- Safe driving app tracking to reduce

Authentication
- Focuses the identity of individuals participating in a certain interaction
- 5 common methods
- Something you know (knowledge factor)
    - Secret word, phrase or factor
    - passwords
- You have (possession factor)
    - Physical item
    - Badge to enter building
    - Smartphones
- You are (inheritance factor)
    - Providing unique characteristic
    - Biometrics
- You do (action factor)
    - Secret handshake
    - Handwriting samples
- Where you are (location factor)
    - Require a certain location
    - Location based factors to allow access to applications
- You can combine factors (MFA - multi factor authentication)
- Authentication used to
    - prevent unauthorized access
        - Bank accounts use proper mechanisms
    - Protect data and privacy
        - Ensuring only being shown to authorized
        - Patient portal for privacy
    - Resource validity
        - Only authorized to certain resources

Accounting

- Ensures all transactions and interactions are recorded
- You have more trust in a more descriptive bank statement
- Good system provides
    - Audit trail
        - Chronological
    - Reg compliance
    - Forensic analysis
        - Help experts
    - Resource optimization
    - User accountability
- Technologies
    - Syslog servers
        - Aggregate logs so they can be analyzed
    - Network analyzers
        - Wireshark
    - SIEM
        - Real time analysis of alerts
- Every action within a system is recorded

Security Controls

- Think as a castle
    - Guards, walls, watchtowers, plans, leader with a strategy
    - Layers give us more protection overall
    - 4
        - Technical controls
            - Technology mechanisms
            - Antivirus software
            - Firewalls
            - Encryptions
            - IDS
        - Managerial Controls
            - Administrative controls
            - Governance side
            - Before moving to the cloud, risk assessment
            - Security policies
            - Training
            - IR strategies
        - Operational
            - Day to day basis
            - Human processes
            - Changing password ev 90 days
            - Backups
            - Account reviews
            - User training programs

        - Physical
            - Real world measures
            - Outside digital realm
            - Fences
            - Scanners
            - Shredding sensitive documents
            - Guards
            - Locks

Security Control Types

- 6 types
    - Preventative
        - Proactive to thwart breaches and threats
        - Firewall
    - Deterrent
        - Discourage attackers
        - Home alarm sign in yard
        - Let bad guy know they're being watched
        - Warning signs
    - Detective
        - Monitor and alert malicious activities
        - Cameras
        - IDS
    - Corrective
        - Mitigate potential damage back to normal state
        - Antivirus software to quarantine and remove malware after detecting it
    - Compensating
        - Alternative measures when primary is not feasible
        - Legacy system cannot support wireless encryption WPA3
            - Use WPA2 and put a VPN on top of it
    - Directive
        - Guide inform or mandate actions
        - Policy or documentation
- Wide range of categories of controls

Gap Analysis

- Process evaluating difference between current and desired performance
- Valuable tool for orgs
- Several steps
    - Define scope
        - Specific areas that will be evaluated
    - Data on on current state
        - Surveys
    - Analyzed to identify gaps
    - Develop plan to bridge gaps
        - Processes or systems

        - Goals objectives
        - Considering security when migrating to the cloud infrastructure
- Two types of analysis
    - Technical
        - Evals current tech infrastructure and ability to utilize sec solutions
    - Business
        - Current business process and where they fall short to utilize cloud-based solutions
        - Develop a plan once identified
- POAM (plan of action and milestones)
    - Outlines measures to address vulnerability allocate resources and set timelines

Zero Trust

- Modern networks cannot simply rely on external defenses only.
- Encryption protocols auth and host based mechanisms
- Deperimeterization has introduced risk to organizations
    - From cloud and work from home
- Trust nothing and verify everything
- Verification for every device, user and transaction
- 2 planes
    - Control
        - Policy and procedures
        - Dictates how when and where access is granted
        - Key elements
            - Adaptive identity
                - One time verif is not sufficient
                - Takes into account behavior device and location
            - Threat scope reduction
                - Limits user to only what they need for their work tasks
            - Policy driven access control
                - User access policy development and management
            - Secured Zones
                - Sensitive data
        - Policy engine
            - Rule book determines whether request matches user permissions
        - Policy administrator
            - Establish and manage access policies
    - Data
        - Subject or system
            - Individual attempting to gain access
            - Verify before granting access
        - Policy enforcement point
            - Access is being granted
            - Gatekeeper to sensitive areas

Threat Actors

- Entity responsible for incidents related to security or data protection
- Can be anyone or anything
- Motivations for Threat Actors
- Threat actor attributes
- Unskilled Attackers
- Hacktivists
- Organized crime
- Nation State Actors
- Insider Threats
- Shadow IT
- Threat vectors and attack surfaces
- How to outsmart threat actors
    - Honey pots
    - Honey nets
    - Honey files
    - Honey Tokens

Threat Actor Motivations

- Understanding what drives them helps us protect our networks
- Difference between intent and motivation
    - Intent - objective or goal
    - Motivation - reasons or driving forces
- Motivations
    - Data Exfil
        - Unauth transfer of data
        - Stealing client contact info
        - Want to access IP or intellectual property
        - Sells it
        - Leverages
    - Financial Gain
        - Most common
        - Ransomware
        - Banking Trojans
    - Blackmail
        - Obtains compromising info and threatens to release unless demands met
        - Financial transaction like bitcoin
        - Ransomware
        - Doxing
        - Sextortion
    - Service Disruption
        - Ddos attack
        - Leads to financial and reputational damage
    - Philosophical or political beliefs
        - Hacktivism
        - Promotes agenda or social change

        - Protest unethical behavior
    - Ethical reasons
        - Authorized hackers
        - Improve sec
        - Pentesters and bounty hunters
        - Identify vulnerabilities in systems and networks to prevent exploits
    - Revenge
        - Employee disgruntled
        - TA wanting to target someone they think has wronged them
    - Disruption or CHaos
        - Unauth hackers
        - For the thrill
        - Cause harm
        - Challenge their skills
    - Espionage
        - Spying on individ
        - Org or nations
        - Gather sensitive or classified info
        - Conducted by nation state actors
    - War
        - Disrupt infrastructure
        - Economic damage
        - Compromise national security
        - Geopolitical objectives
        - Nation state actors

Threat Actor Attributes

- Internal
    - Individuals within an org
    - Uses Legit access to system and data
    - Maybe motivated by revenge, financial gain
- External
    - Outside org
    - Cyber criminals
    - Hacktivists
    - Uses malware and social engineering for access
- Resources and funding
    - Tools skill and personnel
    - Nation state actor can have a ton of resources
- Level of sophistication and capability
    - Skill
    - Complexity of tools and techniques
    - Ability to evade detection
    - Low and high levels of sophistication
        - Low

        - Script kiddie
    - High
        - Advanced skills and tools and techniques
        - Nation state actors

Unskilled Attackers

- Script kiddies - unskilled attackers
    - Still a threat
- Someone who lacks technical knowledge and relies on scripts and programs of others
- Motivated desire of recognition or thrill of disruption
- Motivated by curiosity
- Ddos attack
- Not many resources and skill

Hacktivists

- Promotes cause or drive social gain over financial
- Use hacking to advance political or social cause
- Wide range of techniques
    - Website defacements
        - Like graffiti
    - Ddos
    - Doxing
        - Public release of private information
        - Hoping someone will take action against the victim
- High level of sophistication
- Targets they believe are acting against their cause
- One of the most notorious group - Anonymous
- LulzSec
    - 50 days of Lulz
    - Political motivations

Organized Crime

- Sophisticated and well structured
- Banded together to do criminal activities
- Operate similar to physical organized crime
- Internet gives them anonymity
- High level of capability
    - Custom malware, ransomware, sophisticated phishing
- High level of adaptability
- Exploits technologies
    - Crypto
    - Darkweb
    - Cell collection devices
- Focuses on financial gain
- Variety of illicit activities
    - Data breaches
    - Id theft

        - Fraud
        - Ransomware
    - Not typically driven by ideological or political objectives but may act of activists behalf
    - FIN7
        - Numerous data breaches
        - Advanced phishing campaigns
    - Carbanak
        - Stolen over 1M dollars
        - Sophisticated malware to infiltrate bank systems

Nation-State Actor

- Sponsored by gov
- Against nations, orgs, or individuals
- False flag attack
    - Orchestrated so it seems like it's from another group
- Highly sophisticated
- Extensive resources
- Custom malware, zero day,
- Advanced persistent threat
    - APT
    - Synonymous with Nation state actor
    - Prolonged cyber attack and remains undetected
- One of the mosts dangerous
- Motivated by long term strategic goals
- Wants to achieve political objectives
    - Gather intelligence
    - Disrut infrastructure
    - Influencing Political Processes
- Espionage to steal property or gain advantage
- North Korea
    - Charged with cyber attacks
- Stuxnet worm
    - Attributed to US
    - Sabotage Iranian nuclear program
    - Worm spreads between machines without detection
- Technologically sophisticated state actors are not immune to attacks

Insider Threats

- Originate from within an org
- Current or former employees or associates
- Intimate knowledge of infrastructure
- Already granted access
- Varying levels of capabilities
    - Extensive access privileges can cause significant damage
- Various forms
    - Data theft

        - Sabotage
        - Misuse of privileges
    - Different motivations
        - Financial gain, revenge, carelessness or lack of cyber sec awareness
    - Can be an uneducated employee
    - Edward Snowden
        - Leaked vast amount of info on global surveillance programs without NSA detecting it
    - Twitter Attack of 2020
        - Attacker gains access to high profile accounts
        - Launched bitcoin scam leading followers of these accounts

Shadow IT

- Use of IT resources without org approval
- IT related projects without permission
- Personal devices for work purposes
- Install unapproved software
- Use of cloud services not approved by org
    - Could lead to data leaks or breaches if not managed properly
- Org sec posture is set too high typically
- USB, external devices, etc could be introducing vulns into network
- Can lead to lack of standardization across a network
- Employees want to gain efficiency
    - Plugins and extensions
- BYOD
    - Your own devices
    - Convenience but potential to risk
    - IT doesn't own or proctor them
- Significant challenge for organizations

Threat Vectors and Attack Surfaces

- Threat Vector
    - Means or pathway to access a network for unwanted action
- Surface (where of attack)
    - Points where data can be extracted or entered from an environment by an unauth user
    - Sum of all vuln and entry points
    - Minimized by
        - Restricting access
        - Removing unnecessary software
        - Disabling Unused protocols
- Messages
    - Email, SMS, instant messaging
    - Attacker impersonated someone trusted to get sensitive info
    - Malicious links
- Images

        - Embedding malicious code in an image file
        - Executed when opened
        - Stegano
            - Within banner ads on websites
            - Older internet Explorer browser
            - Hosts exploit kit attempts to installs malware on hosts
- Files
    - Email attachments
    - Hosted on malicious website
- Voice Caslls
    - Vishing
    - Try to impersonate trusted to get sensitive info
    - IRS scams to scare people to get their info
- Removable devices
    - USBs
    - External storage devices
    - Baiting
        - Leave drive where someone can find it
        - Target plugs it in and installs malware
    - Social Engineering
- Unsecured Networks
    - Wireless, wired, and bluetooth
    - Intercept data
    - Get access to devices
    - Wireless
        - Attackers can set up rogue access points (fake wifi)
        - Attackers intercept wireless communications
    - WIred networks
        - More secure
        - Not immune to threats
        - Taps into cables
        - Mac address cloning
        - VLAN hopping
    - Bluetooth
        - Exploits vulns
        - Blueborn exploits
            - Vulnerabilities in bluetooth tech
            - Allow takeover devices and spread malware
        - BlueSmack
            - Type of DOS attack
            - Sends logical link control and adaptation protocol packet to a device
            - Consume all resources and cause to crash

Outsmarting Threat Actors

- Deception and Disruption technologies
    - Honeypots, honey nets, honey files, honey tokens
    - Mislead, confuse, and divert attackers from assets while simultaneously detecting and neutralizing them
    - Honey Pots
        - Decoy system
        - Mimic real system
        - Gather info on attacker motives, TTPs, etc
        - Logs all interactions
        - Locate within an isolated segment that can be easily accessed
    - Honeynet
        - Complex system
        - Mimic entire network
        - Logs all activities
        - Provides wealth of data
    - Honey Files
        - File system to lure attackers
        - Trap
        - Fake data
        - Alert triggers and notifies intrusion
        - Some have code to allow enumeration of attackers network
        - Word docs, spreadsheets, database files, images, executable files
    - Honey Tokens
        - Data or resource
        - Fake user account, url, database record
        - Useful for detecting insider threat
    - Some D&D technologies can be used to secure networks
        - Fake DNS entries
            - Admins can mislead attackers to waste their time and resources
        - Decoy Directories
            - Fake folders and files
            - Alarms can trigger
        - Dynamic page generation
            - Confuse and slow attacker
            - Effective against bots and scribe tools
        - Port Triggering
            - Specific ports remained closed until outbound traffic pattern is detected
            - Ensure certain services are available to certain users when needed
        - Fake Telemetry
            - System can send fake telemetry once alarmed on an attacker being present
            - Confuses and wastes hackers time

        - Ex. telemetry can say the wrong OS type to prevent the right malware from being installed on the system
- TTPs
    - Specific method, patterns, or behaviors of threat actors
    - Used to anticipate cyber attacks and threats