C836 Notes:

**Information Security**: protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction

**Verification**: act of verifying your identity i.e. SSN, Birth Certificate, ID,

**Logical security**: passwords, authentication, access controls

Sandbox: isolated environment that protects a set of resources

1. **Security Tools**
   1. Wireshark
   2. Volatility
   3. Nitko
   4. Nmap
2. Enables users to connect from an untrusted network and encrypt the network traffic
   1. ANSWER
3. **Network Security Solutions**
   1. VPN
   2. DMZ
   3. IDS: intrusion detection system
   4. PKI
4. **Security Principles**
   1. Application
   2. Operations
   3. Human Element
   4. Physical
5. **Security Protocols**
   1. Telnet
   2. SFTP
   3. HTTPS
   4. S/MIME
   5. SIEM
6. **Children Online Privacy Protection Rules (COPPA)**
   1. Mandatory Industry
   2. Optional Industry
   3. Federal regulatory
   4. State regulatory
7. **Compliance Guidelines** 
   1. HIPPA: healthcare and patient records
   2. PCI DSS: Payment Card Industry data
   3. FERPA
   4. SOX
   5. FISMA: defines security standards for federal agencies
8. **Website Protection Measures** 
   1. Hashing
   2. Captchas: control access based on whether party can pass a test- i.e., Turing test to tell humans and computers apart
   3. Tokens: physical USB like security devices
   4. Certificates

1. **CIA Triad**
   1. C*onfidentiality*: refers to our ability to protect data from those who are not authorized
   2. *Integrity*: ability to prevent people from changing data in an unauthorized or undesirable manner
   3. *Availability:* refers to the ability to access our data when we need it
2. **Parkerian Hexad (includes 3 elements of CIA)**
   1. *Possession:* physical disposition of the media on which the data is stored
   2. *Authenticity:* attributed the data in question to the proper owner/creator
   3. *Utility:* how useful the data is
3. **Types of attacks**
   1. *Interception:* Attacks confidentiality takes on the view of unauthorized access
   2. *Interruption:* make assets unavailable to you
   3. *Modification:* tampering an assets
   4. *Fabrication:* generating data, processes, communications
   5. Cross-Site request forgery (CSRF): an attack that misuse the authority of the browser on the user’s computer
   6. *Clickjacking:* interface redressing attacker takes control of some portion of the website that a client would normally click
   7. *Confused Deputy Attack:* The software with access to a resource (the deputy) has a greater level of permission to access the resource than the user who is controlling the software – tricking the software
   8. *Distributed Denial of Service:* hacker control multiple systems remotely and uses them to launch an attack on a server or network
4. **Triple AAA**
   1. *Authentication:* verifies identifications via process of logging into a system
      1. Multifactor:uses on or more different factors to log into a system
      2. Mutual:both parties authenticate each other in a transaction (typically software based)
         1. *Authentication Methods:*
            1. Passwords
            2. Biometrics: fingerprints etc.
            3. Hardware tokens*:* looks like a USB and contains a certificate of unique identifier; complex ones contain LCD (liquid crystal displays called dongles)
   2. *Authorization:* Determines what a user has the authority to do and have access to
      1. *Access Control:* Anything that allows or denies access
         1. Access control lists (ACLs): lists contain information about what kind of access certain parties are allowed to have given to a system. Can be seen in app software, operating systems, and in firmware of some hardware appliance, such as network infrastructure devices
            1. *File System ACLs*

Read:allows user to access contents

Write*:* allows user to write a file or directory

Execute*:* allow user to execute the contents of the file if it contains a program or a script capable of running on the system

* + - * 1. *Network ACLs:* filters access based on IP address. Media Access, Control Addresses and ports

Media Access Control*:* address filtering which are unique identifiers hard coded into each network interface

IP Address Control: Deny access to a particular IP address

* + - * 1. Capabilities:/capability-based systems: right to access a resource based entirely on possession of a token, rather than who possess it -with whatever permission is placed on it
  1. Accounting: Tracks and records user access and action with system logs
  2. Access Control Models
     1. Discretionary Access Control (DAC): the owner of the resource determines who gets access and what level of access – implemented I most operating systems
     2. Mandatory Access Control (MAC): the owner does not get to decide who gets access to it – separate group or individual authority set access
     3. Rule-Based Access Control: allows access according to a set of rules defined by the system administrator
     4. Role Based Access System (RBAC): allows access based on the role of the individual
     5. *Attribute-Based Access Control (ABAC):* based on the specific attributes of a person, resource, or environment
        1. Subject Attributes: belongs to induvial – ie. height
        2. Resource Attributes: belong to resource, i.e., operating system or application & requiring certain programs ran on certain software
        3. Environmental attributes: enable access controls based on environmental conditions - i.e., time
     6. *Multilevel Access Control*: combine several of the access control models
        1. Bell-LaPadula: implements DAC & MAC, concerned with confidentiality -focusing on unauthorized people can’t use it
        2. Biba Model: primarily concerned with protecting the integrity of data, even at the expense of confidentiality
        3. Brewer and Nash (Chinese Wall): prevents conflict of interests, sensitive data
     7. Physical Access Controls: controlling movement of induvial and vehicles – regulates movement

1. **Least Privilege:** user system, process, or application is only given permission necessary to complete assigned tasks or function and nothing more
   1. *Security Groups:*
   2. *Account Standardization*
   3. *Account Management Processes & Procedures*
2. **Risk Management:** identifying, assessing, monitoring, and limiting risk to an acceptable level
   1. *Asset:* composed of ppl property, information
   2. *Threat:* anything that can exploit a vulnerability
   3. *Vulnerability:* a weakness of an asset exploited by a threat
   4. *Risk:* potential for loss, damage, or destruction of an asset
      1. *Equation:* Risk = Threat x Vulnerability
   5. *Process for Risk Assessments:*
      1. Identify, Assess, Assign, respond
         1. ***Qualitative Assessment*** 
            1. *Probability****:*** likelihood
            2. *Impact:* negative impact if risk occurs
   6. *Risk Categories* 
      1. Avoidance*:* The process of eliminating a risk by not engaging in that activity
      2. Acceptance*:* accepting an identified risk, meaning no action will be taken
      3. Mitigation*:* process of taking steps to minimize impact
      4. Transference*:* transferring responsibility of risk to a 3rd party
      5. Residual Risk*:* risk that remains after transference risk activities have taken place
3. Data Security
   1. *Layer 1-Physcial Security*: protection from physical threats
   2. *Layer 2 -Network Security*: protection to a network and its services
   3. *Layer 3- System Security*: protection to a system and its data from unauthorized access
   4. *Layer 4- Application Security*: protection to the applications
   5. *Layer 5- User Security*: provides authentication to a system or network
   6. *Data Masking:* hides data by concealing letters and numbers with different characters
   7. *Encryption:* data that can only be read by authorized user