SECURITY+ Notes

- Chapter 1 – Mastering Security Basics
  - Use Case - describes a goal that an organization wants to achieve
    - Important to identify and clarify requirements
  - Elements of Use Case Systems:
    - Actors, Preconditions, Postconditions, Triggers, Normal Flow, Alternate Flow
    - Common Use Cases related to supporting confidentiality, integrity, availability, authentication, obfuscation, and non-repudiation.
  - Ensure Confidentiality – prevent unauthorized disclosure of data
    - Encryption – best way to protect PII in storage and transit
    - Access Controls
      - Identification, Authorization, and Authentication combined
      - Usernames, passwords, permissions respectively
    - Steganography and Obfuscation
      - Hide data within data
      - Security through obscurity is a commonly rejected concept
  - Provide Integrity
    - Provide assurance that data has not changed (modification, tampering, corruption)
    - Hashing
      - Does not tell what or how content was modified, only that it was
      - Message authentication codes (MAC) used to compare hashes developed at two separate times for same value
    - Digital Signatures, Certificates, and Non-Repudiation
      - Commonly used with email
      - Prevents impersonation
      - Audit logs another method – record what, where, who, when
      - Digital Signatures require use of Certs and Public Key Infrastructure (PKI)
        - To create, manage, distribute certs
  - Increase Availability
    - Data/Services when needed
    - Redundancy and fault-tolerance, duplication of critical systems
    - Remove Single Points of Failure (SPOF)
    - Common Strategies:
      - Disk Redundancy – RAID 1, 5, 10
      - Server Redundancy – Failover Clusters, VMs
      - Load Balancing – multiple servers per service
      - Site Redundancy – offsites (hot, warm, cold)
      - Backups
      - Alternative Power – UPS, Generators
      - Cooling Systems – HVAC
    - Patching
      - Patch Management Programs
  - Resources Versus Security Constraints
    - Balancing Act
    - Minimize cost w/o sacrificing security
  - Introducing Basic Risk Concepts
    - Reduction of risk by identifying threats and exploits/vulnerabilities and prevent security incidents
      - Such as intentional attacks, infections, accidental data loss, etc.
    - Threats can be internal, external, natural, intentional, accidental

        - Reduce risk through mitigation
            - Countermeasures, safeguards as controls
    - Understanding Control Types
        - Technical, Administrative, Physical = Implementation Types
        - Preventative, Detective, Corrective, Deterrence, Compensation = Actual Security Control Goals
        - Majority of Security Controls fall under Three Implementation Types
    - Technical Controls
        - Reduce Vulns
            - Encryption, IDS/IPS, Firewalls, Least Privilege, Motion Detectors, Fire Suppression
    - Administrative Controls
        - Mandated by Organization policies and guidelines
        - Assessments to provide ongoing review of an organizations risk management capabilities
            - Risk assessments – CBAs, probability, impact
            - Vulnerability Assessment – discover current vulns and weaknesses
                - Highlights need additional implementation of controls
            - Penetration Testing
                - Test/exploit defenses and vulns
        - Operational and management controls
            - Awareness training, configuration and change management, contingency planning, media protection, physical and environmental controls
    - Physical Controls
        - Lighting, fences, signs, security guards, environmental controls
    - Control Goals
        - Classifying security controls based on how they are implemented and their relationship to security incidents
        - Preventative, detective, corrective, deterrent, compensating
        - Preventative
            - Hardening – system becoming more secure than default config
            - Defense in depth
                - Disable ports and services, secure protocols, strong passwords, disable default accounts, account disabling policy
                - Security awareness and training, change management process
                - Security guards
        - Detective Controls
            - Detect when exploits occur
            - Log Monitoring
            - Trend analysis via IDS
            - Security Audit
            - Video Surveillance – CCTV
            - Motion detection
            - DIFFERENCE BETWEEN DETECTION AND PREVENTION
        - Corrective Controls
            - Reverse impact of an incident
            - IPS
            - Backups and system recovery
        - Deterrent Controls
            - Cable locks, guards, hardware locks

        - Overlaps with preventative
    - Compensating Controls
        - Time-based one-time use passwords
        - Temporary holdovers while primary controls are being applied
    - Combining Types and Goals
        - Overlap between different categories, not mutually exclusive
- Implementing Virtualization
    - Hypervisor
    - Host + host elasticity and scalability
    - Guest
    - Typically provides best ROI when organizations have underutilized servers
    - Comparing Hypervisors
        - Type 1 – run directly on system hardware; bare-metal; no OS
        - Type 2 – run as software within host OS
    - Application Cell or Container Virtualization
        - Services/apps run within isolated application cells
        - Host OS + kernel run a service or app within each container which cannot interfere with one another
            - Uses fewer resources and can be more efficient than standard Type 2
            - Commonly used by ISPs
                - Must share same OS type
- Secure Network Architecture
    - Provide segregation, segmentation, and isolation of individual systems
        - Disable VM NIC
    - Snapshots
        - Provide backups for reversion in case changes are not successful
    - VDI/VDE and Non-Persistence
        - Virtualized Desktop Infrastructure/Environment
            - Desktop runs as VM on a server
            - Allows PCs to have limited hardware resources
            - Persistence allows customizable virtual desktops that can save data
            - Non-Persistence saves a uniform desktop to all users that is reset upon logoff
    - VMs as Files
        - Virtual servers can be moved around for space considerations
        - VMs are also easily restored vs a physical server
        - Multiple virtual systems can be run on a single server (even with different hosts)
            - Single management interface
    - Risks associated with virtualization
        - VM Escape
            - Attack that allows host sys to be accessed from within VM
                - Code allows interaction with hypervisor
                - Gives attacker elevated privilege
            - Mitigated with patches
        - VM Sprawl
            - Poorly managed VMs
                - Unauthorized added resource load
                - Blind gaps in security if machines go unattended, forgotten, unpatched
        - Loss of confidentiality
            - Much easier to steal

        - Running Kali Linux on VM
            - HyperV, VMWare Workstation Player, OracleVM
    - Using Command Line Tools
        - Windows Command Line
        - Linux Terminal
        - Understanding Switches and Getting Help
            - Windows – forward slash or dash (-?; /?)
            - Linux – dash (-?)
        - Understanding Case
            - Windows – not case sensitive
            - Linux – is case sensitive
        - Ping
            - ICMP echo request packets
                - Continuous on Linux until Ctrl + C or ping -c
                - 4 packets with Windows unless ping -t
        - Using Ping to check Name Resolution
            - Ping hostname of a remote system and verify that name resolution is working
            - As DoS attacks use ICMP, Firewalls often block ICMP traffic
        - Using Ping to Check Security Posture
            - Using ping from several sources to test if firewalls and IPS systems will block sudden ICMP flows
                - Verify that routers, firewalls, and IPS block ICMP traffic when configured to do so
        - Ipconfig, ifconfig, and ip
            - Ipconfig shows TCP/IP configuration info for a system
                - NICs, MAC, subnet, Default Gateway, IP, DNS, etc.
            - Linux uses ifconfig for non-Debian distros (use ip)
                - Can configure NICs w/Linux
                - Promiscuous/non-promiscuous mode
        - Netstat
            - System TCP/IP protocol statistics, active connection view
            - States of connections
                - Established – data transfer phase, active/open
                - Listen – waiting for connection req
                - Close-wait – waiting for connection termination req
                - Time-wait – waiting for remote system receipt of TCP based acknowledgement
                - Syn-Sent – TCP SYN sent, awaiting SYN-ACK
                - SYN-Received – SYN-ACK sent, awaiting ACK, excessive amount may indicate SYN attack
            - Tracert and Traceroute (Linux)
                - Lists routers between two systems via hops
                    - IP address, host name, RTTs
                - Identify faulty routers or modified paths (security)
                    - Valuable when troubleshooting issues through a WAN
                    - ID unauthorized routers or modified internet paths
            - ARP
                - Address Resolution Protocol
                    - Arp command allows user to view and manipulate the ARP cache
                        - ID MACs of machines on local networks

- Exploring Authentication Concepts
    - Authentication proves an identity via credential
        - Identification plus authentication is critical for access controls
    - Comparing Identification and AAA (Authentication, authorization, accounting)
        - Work with identification for comprehensive access management
            - Authorization allows for access to a given set of resources
            - Accounting tracks user activity and records it
        - Create audit trails via logs
        - Strong authentication is the core
    - Comparing authentication factors
        - Something you know (PIN, password) – passphrases best
    - Training users about password behaviors
        - Password expiration
            - 45-90 days
        - Password recovery
            - Verify ID, change to temp
            - ID-proofing system
            - Prevent re-use of old passwords
        - Group Policy
            - Sys admins configure settings for multiple users/computers in a domain via Group Policy Objects (GPO)
                - Active Directory Domain Services
        - Using a Password Policy
            - Written document with stated goals and specifics concerning passwords
            - Implemented technically with a technical password policy in a GPO
                - Enforce history, max/min age, min length, complexity
                - Store with reversible encryption
        - Implementing account lockout policies
            - Preventing excessive password guessing
                - Account lockout threshold and duration
        - Changing default passwords
            - Passwords, names
            - Dummy false admin accounts
    - Something you have
        - Something physically held
            - Smart cards
                - Provides confidentiality, integrity, authentication, and non-repudiation
                - Requirements
                    - Embedded certificates
                    - PKI
                - Used in conjunction with another form such as a PIN
            - CACs and PIVs
                - Common Access Card
                    - Used by DoD
                    - Picture and additional info
                - Personal Identity Verification
                    - Federal agencies
                    - CIA + non-repudiation
                - Both support 2FA
            - Tokens and Key FOBs
                - Hardware, logical, software tokens

        - Random numbers and synced with server
            - OUT rolling password
        - Used for authentication
            - RSA SecureID
    - HOTP and TOTP
        - Hash-Based Message Authentication Code (HMAC)
            - HMAC-based One-time password (HOTP)
                - Open standard for creating one-time passwords
                - Uses a secret key and an incrementing counter which produces a hash
            - Result then converted into an HOTP value of 6-8 digits
                - Password remains usable forever until its first use
                    - Still has potential security risks
        - Time-based One-Time Password
            - Similar to HOTP
            - Uses timestamp rather than a counter (30 sec average)
        - Both are open source, allowing for inexpensive use of hardware tokens based on these systems
- Something You Are
    - Geolocation via IP
        - Can be fooled via VPN IP address changers
    - MAC address
- Something You Do
    - Actions taken, like gestures
    - How you write, how you type
        - Keystroke dynamics
    - Behavioral dynamics, biometrics
- Dual-Factor and Multifactor Authentication
    - 2 vs 2+

- Summarizing Identification Methods
    - Usernames, photo ID, biometrics
- Troubleshooting Authentication Issues
    - Weak passwords, forgotten passwords
    - Biometric errors
- Comparing Authentication Services
    - Ensure that authentication credentials are not sent across a network
    - KERBEROS
        - Network authentication mechanism used within Windows Active Directory domains and Unix realms
        - Mutual authentication to prevent man-in-the-middle attacks and tickets to prevent relay attacks
        - Requires
            - Method of issuing tickets used for authentication (Key Distribution Center [KDC]) for ticket-granting tickets (TGTs)
            - User credentials are packaged within a ticket
                - Provides authentication for users when they access resources (logical tokens)
            - Time synchronization within 5 minutes of all systems involved
                - Prevents replays
                - A database of subjects of users
                - KDC tickets have a 10 hour timestamp

- NTLM
  - New technology LAN manager
    - Protocols that provide authentication, integrity, and confidentiality with Windows
  - Use message digest algorithm to challenge and check user credentials
  - NTLM s/ MD4 – cracked and unsafe
  - NTLM v2 – challenge response with HMAC-MD5 hash of username – computer/domain name – password – time – etc
  - NTLM2 Session – improves NTLMv2 by adding mutual authentication
    - Negotiate security package is automatically setup – KERBEROS or NTLMv2/NTLM2 Session
- LDAP and LDAPS
  - Lightweight Directory Access Protocol specifies formats and methods to query directories (databases with central access point)
    - X.500 extension
  - Active Directory is based on LDAP
  - LDAP Secure uses encryption to protect LDAP transmissions with TLS
- Single Sign-on
  - Credentials provided only once, as SSO creates a secure token for that singular logon session
  - Requires strong authentication
- SSO and Transitive Trust
  - Indirect trust relationship can help reduce network and administration
    - LDAPS use transitive trust for SSO
- SSO and SAML
  - Security Assertion Markup Language is an XML based data format used for SSO on browsers
    - Federated identity management system between two organizational sites
  - Commonly used on web-based portals
  - SAML defines three roles
    - Principle – user
    - Identity Provider – creates, maintains, manages ID for principle
    - Service Provider – provides services to principles
- SAML and Authorization
  - Primary purpose of SSO is for identification and authentication of users
  - SSO does not provide authorization, but does include the ability to transfer authorization data between their systems
- SSO and a Federation
  - Same SSO systems can connect with authentication mechanisms from other environments (operating systems, networks)
    - Federated Identity Management System
      - Provides central authentication in a non-homogenous environment
      - A federation requires a FIDM system that all members of the federation use
        - Shibboleth – open source with open SAML libraries
- OAuth and OpenID Connect
  - Open standard for authorization many companies use to provide secure access to protected resources
  - OpenID Connect works with OAuth2.0 to verify ID of end users without managing credentials

- Managing Accounts
  - Creation, management, disablement, and termination of accounts

        - When active – access controls are used to control what a user can do, when, and where
    - Least Privilege
        - Individuals and processes are granted only the rights and permissions needed to perform relevant tasks
        - Reduce risk, applies to all users and admins
        - Many services and applications run under user account context – deriving privileges from said account
        - Focus on both rights and privileges
    - Need to Know
        - Users granted access only to data and information needed to know for their job
        - Focus on data and information
    - Account Types
        - End User Accounts – regular users
        - Privileged Accounts – additional rights and privileges beyond what regular users have
        - Guest Accounts – limited access without a new account being created
        - Service Accounts – accounts assigned appropriate privileges relevant to the task and us used by a service or application, not an end user
    - Require Administrators to use Two Accounts
        - One for regular use, another with elevated privileges for admin work
    - Standard Naming Convention
        - Ensure user account names and email addresses are created similarly
        - Be sure to understand and adhere
    - Prohibiting Shared and Generic Accounts
        - If multiple users share an account, you cannot implement basic authorization controls
            - Lose IAAA
    - Disablement Policies
        - Specifies how to manage accounts in different situations
        - Disable default accounts, accounts of users no longer with organizations
        - Disablement is preferred in the short-term over deletion
    - Recovering Accounts
        - Enable a disabled account
        - Recover a deleted account
    - Time of Day Restrictions
        - Set time that an account is accessible
    - Location based policies
        - Geolocation tech via IP
        - Block unacceptable addresses
        - Black and White lists
        - Within a network, restrict access via MAC
    - Expiring Accounts and Recertifications
        - Accounts can be set to expire automatically, requiring recertification
            - Common for temporary accounts
    - Account Maintenance
        - Scripts to automate
            - Usage, inactivity, ability, status, etc.
    - Credential Management
        - Credential manage systems help users to store collections of info used as certification securely
        - Simplify management, limit unauthorized access
            - Credential Manager (windows)
- Company Access Control Models

- Role-Based Access Control (Role-BAC)
  - Uses roles to manage rights and permissions, such as in a specific department or a specific job function
- Using R-BAC on Jobs and Functions
  - Create roles that reflect departments, jobs, or functions
    - Assign roles to members and levy access to server
  - Project managers
    - Admins, execs, project managers, team members
- Documenting Roles Within a Matrix
  - It is common to document R-BAC permissions with a matrix listing all of the job titles and the privileges for each
  - Can also be hierarchy, job, task, or function based
- Establishing Access with Group-Based Privileges
  - Roles are often implemented as groups
  - Can be reflective of organizational structure
    - Rights and privileges are assigned to groups and users are added to groups
  - Simplifies user administration
    - Microsoft built-in security groups like Administrators
- Rule-Based Access Control
  - Rules in firewalls and routers, even within applications
    - Rules used within access control lists which define what traffic devices allow into network
      - Static rules
      - Dynamic rules (IPS)
- Discretionary Access Control
  - Every object has an owner, and the owner establishes access for the object
  - New Tech File System (NTFS) in Windows
    - Allows users and admins to restrict access to files and folders with permissions
- SIDs and DACLs
  - Users identified with security identifiers (SIDs)
  - Every object has a discretionary access control list (DACL) that IDs who can access it in a system
    - List of Access Control Entries, each ACE is comprised of a SID and Permissions granted to that SID
  - The Owner Establishes Access
    - File creators are also the owners, with explicit control
      - Modify permissions via user and group accounts
    - More flexible than MAC model
  - Beware of Trojans
    - DAC is susceptible to Trojans as file downloads will have the users privileges
  - Mandatory Access Control
    - Uses sensitivity and security labels to determine access
      - Labels assigned to both subjects and objects
    - Matching labels = access granted
    - Popular in military
      - Used in conjunction with need to know
      - Security-enhanced Linux (SELinux)
  - Labels and Lattice
    - Levels of security are defined in a lattice
      - A complex relationship between different ordered sets of labels
    - These labels define boundaries

        - Establishing Access
            - Admin responsibility but only someone at a higher authority
                - ID specific access
                    - Upgrade/downgrade
            - Multiple approval levels involved in decision making process
    - Attribute-Based Access Control (ABAC)
        - Evaluate and grants access based on value of attributes (characteristics of a user)
        - Many software-defined networks (SDNs) used ABAC
            - ABAC system policies control traffic, not the router itself
        - Four Elements
            - Subjects
            - Objects
            - Action
            - Environment
        - ABAC is flexible, capable of enforcing DAC or MAC

Chapter 3 – Exploring Network Technologies and Tools

- Reviewing Basic Networking Concepts
- Basic Networking Protocols
    - Provide Rules needed for computers to communicate with each other on a network
    - TCP/IP, HTTP, SMTP
    - TCP/IP is a suite of protocols with well-known ports
        - Ports are critical knowledge when implementing ACLs in routers and stateless firewalls, and disabling unnecessary ports and services
    - TCP
        - Three-way handshake protocol, connection-oriented
    - UDP
        - Connectionless sessions, ICMP and audio/video streaming
    - IP
        - IDs hosts in TCP/IP network with IPv4 and IPv6 addresses
    - ARP
        - Resolves IPv4 to MAC, requested once packet reaches destination subnet
    - NDP
        - IPv6 functions like IPv4 ARP.
        - Also performs IPv6 autoconfiguration and IPv6 device discovery
- Implementing Protocols for Use Cases
    - ID a need based on an organization goal and enable best protocol to meet that need
    - Voice/Video Use Case
        - UDP, Real-Time Transport Protocol (RTP), (VoIP)
        - Secure Real-Time Transport Protocol (SRTP) provides encryption and message authentication and integrity
            - Confidentiality while ensuring integrity
                - Prevent replay attacks
            - Unicast and multicast use
    - File Trans Use Case
            - Transmitting data over a network
            - Ensuring confidentiality
            - Ensuring admins can connect to servers
            - Using secure connections
        - FTP – upload and download large files to and from an FTP server
            - Cleartext, Port 21 TCP (Control)
                - Port 20 TCP (Data)

        - Passive FTP, Port 21 TCP (Control)
            - Random TCP port for data
            - Often blocked by firewall
    - Trivial FTP
        - UDP Port 69
            - Smaller amounts of data
        - Commonly disabled
    - SSH
        - Encrypts traffic and other protocols
        - Secure copy (SCP) based on SSH for encrypted file copy
        - Encrypt TCP wrapper (for ACL uses) at TCP port 22
    - SSL
        - No longer recommended
    - TLS
        - Replaces SSL for HHTPS, SMTP, LDAP via STARTTLS command
    - IPsec
        - Encrypts IP traffic
        - Native IPv6 support
        - Encapsulates IP packets via VPN tunneling
            - Uses Authentication Header (AH) protocol ID #51 and Encapsulating Security Payload (ESP) with PID #50
        - IKE over UDP port 500 for VPN security association
    - SFTP
        - Secure implementation of FTP via SSH TCP port 22
    - FTPS
        - Extension of FTP via TLS
        - TCP ports 989 and 990 or FTP ports 20 and 21
- Email and Web Use Cases
        - Send/receive email, secure email
        - Manage email folders
        - Internal access to external web or external web access to internal organizational resources
        - Common support for STARTTLS
    - SMTP – TCP port 25, clients ←→SMTP servers
    - POP3 and Secure POP – TCP port 110, servers → clients
    - IMAP4 and Secure IMAP – TCP port 143, storage of emails on an email server
        - Organize and manage emails in folders on a server
    - HTTP
        - Inter/intranet traffic
        - TCP port 80
        - HTML language
    - HTTPS
        - SSL/TLS TCP port 443
- Directory Services Use Case
        - Streamline management and implement security
        - Secure network access
        - Active Directory Domain Services
    - KERBEROS
        - UDP port 88
    - LDAP

        - TCP port 389
        - LDAPS TCP port 636
    - Group Policy – GPOs exist within domain
- Remote Access Use Cases
    - Remote admin/user access
    - Often SSH
        - Netcat + SSH (Linux)
    - Remote Desktop Protocol (RDP)
        - TCP port 3389 (More common) or UDP port 3389
        - Can be blocked via host-based network firewall
        - VPN alternative
- Time Synchronization Use Case
    - Network Time Protocol
    - KERBEROS use
    - Single NTP server, domain controller sync to NTP server, computers syn within each domain
        - SNTP can be used, but less accurate
- Network Address Allocation Use Case
    - DHCP
    - IPv4
        - 32-bit, dotted decimal
        - Internet IPs – public addresses
        - Internal Ips – private addresses
        - RFC 1918
    - IPv6
        - 128-bit, hexadecimal, colons (fc00)
        - Unique local addresses instead of private Ips
- Domain Name Resolution Use Case
    - DNS
        - Servers host data in zones
            - A – host record = host name + IPv4 address
                - Most commonly used
                    - Queried with Forward Lookup Address
            - AAAA – hostname + IPv6 address
            - PTR
                - Pointer Record
                - Opposite of A
                - DNS client queries DNS with IP address, not name
                    - Optional, does not always work
            - MX – Mail eXchange
                - Used for email
                - Linked to A/AAAA
            - CNAME – canonical names allow a single system to have multiple names associated with a single IP address
            - SOA – State Of Authority
                - DNS zone info
                - TLS settings
        - Most DNS servers run BIND on Unix/Linux servers
            - Zone transfers use TCP port 53 whereas Name Resolution uses UDP 53
- DNSSEC
    - Risk of DNS poisoning, modifying DNS cache with false IP addresses

- Prevented with DNS Security Extensions (Digital signature address to each record that provides data integrity)

- Nslookup and Dig
  - Nslookup is used to troubleshoot DNS related problems
    - Verify DNS resolution or FQDNs
  - Dig command line replaced nslookup on Linux
    - Domain information groper
    - Query DNS servers, verifying records and responses
      - Uses @ to specify target server
- Subscription Servers Use Case
    - Commonly use HTTPS with database servers with TLS connections
- Understanding and Identifying Ports
  - Logical numbers used by TCP/IP to ID services and applications to handle data received by a system
    - TCP – 0-65,535
    - UDP – 0-65,535
  - Admins open ports on firewalls/routers to allow associated protocols into/out of a network
    - Also disable unnecessary ports and services (basic security)
  - IANA
    - Well-known ports – 0-1023
    - Registered ports – 1024-49,151
      - Companies
    - Dynamic and Private Ports – 49,152-65,535
      - Used by any application to temporarily map an application to a port (ephemeral ports)
      - Most attacks are levied against well-known ports
        - Use port scanners
        - Common: 20, 21, 22, 23, 25, 80, 443
- Combining the IP address and the Port
  - Packets include destination IP address and destination port
    - Ensures correct application/service on correct host receives and handles packet
- IP Address Used to Locate Hosts
  - TCP/IP uses IP addresses to get packets from computer to web server and response back to client
- Server Ports
  - Port 22 = SSH
  - Port 25 = SMTP
  - Port 80 = HTTP
  - Port 443 = HTTPS
  - Popular web servers include Apache and Internet Information Systems (IIS)
- Client Ports
  - TCP/IP works with client OS to maintain a table of client-side ports
    - Starts at 49,512-65,535
    - An unused port will be recorded by client to be used to handle return traffic from a page request
- Putting It All Together
  - When entering a URL for a webpage via browser
    - Host creates a packet with source and destination IP addresses and ports
      - DNs server is queried for IP address of URL
        - For example, HTTP destination port is 80

        - Host ID's unused port in dynamic and private ports range and map port to browser
            - TCP/IP uses destination IP to get to webpage server
                - Server creates return packets, swaps destination and source IPs and sends packets to newly designated port
- The Importance of Ports in Security
    - Control protocol traffic via routers/routing component of firewalls
        - Open and close ports
- Understanding Basic Network Devices
        - Common use case for a switch is to connect hosts together within a network
        - Common use case for a router is to connect multiple networks together
        - IPv4 uses either unicast or multicast
    - Switches
        - Can learn which computers correspond to each of its physical ports
            - Creating internal switched connections
    - Security Benefit of a Switch
        - Unicast traffic cannot be read by a port analyzer if it is not one of the specified ports
        - Traditional hubs shared all traffic, making it readable by a third party
    - Port Security
        - Limits the computers that can connect to physical ports on a switch
        - Address (MAC) filtering is another method
    - Physical Security of a Switch
        - Console/monitoring ports see all traffic, therefore a switch must be physically protected from attackers attempting to jack in
    - Loop Prevention
        - Spanning Tree Protocol (STP) or newer Rapid STP (RSTP)
    - Flood Attacks and Flood Guards
        - Overload a switch with different MAC addresses associated with each physical port
        - Large amount of traffic with spoofed MAC addresses to same port
            - Runs out of memory causing a fail-open state
                - Switch become a hub
        - Flood Guard prevents these attacks
            - Limiting MAC storage memory
            - Exceeding limit sends an alert with a Flood Guard sending an SMTP trap/alert
                - Restricts/disables port
            - Max number of MACs support by a port
    - Routers
        - Connects multiple network segments together into a single network and routers traffic between segments
        - Routers do not pass broadcasts, reducing segment traffic
            - Broadcast domains (Subnetting)
    - Routers and ACLs
        - Provide rule-based management for the router and control inbound/outbound traffic
        - Basic packet filtering via IP addresses, ports, protocols, encrypted/cleartext
    - Implicit Deny

        - All traffic that isn't explicitly allowed is implicitly denied
            - ACLs and Firewalls
    - Anti-spoofing
        - Modify access list to allow/block IP addresses
            - Blocking private IPs arriving over the internet
- Bridge
    - Connects multiple networks together and can be used in place of a router (sometimes)
    - Directs traffic based on destination MAC address
        - Segments within a subnet
    - Learns MAC addresses with traffic analysis
- Aggregation Switch
    - Connects multiple switches together in a network
        - Reduces number of ports used in a router
- Firewalls
    - Filters incoming/outgoing traffic, blocks downloads
        - Simple packet to advanced content filtering
        - Implicit deny rule
- Host-based Firewalls
    - Single-host monitoring (server or workstation)
    - Monitors NIC traffic, preventing intrusions
    - Linux xtables allow rule configuration (functional ACL)
    - Used in conjunction with network firewall for defense in depth
- Application-Based Versus Network-Based Firewalls
    - App-based → software (Like host-based)
    - Network-based → dedicated hardware and software
        - 2+ NICs with all traffic passing through
        - Firewall controls traffic
    - Stateless Firewall Rules
        - ACLs rules used to ID allowed/blocked traffic
            - Format
            - Permission – Permit/Allow or Deny
            - Protocol – TCP or UDP, or IP (both), ICMP
            - Source – Source IP, any/all
            - Destination – Destination IP, any/all
            - Port – port number, symbol. Value
    - Stateful Versus Stateless
        - Stateful inspects traffic and makes decisions based on context/state of traffic
        - Tracks sessions and inspects session states
        - Any traffic not part of a session is blocked
        - Common issue can be misconfigured ACLs
    - Web Application Firewall
        - Specifically designated to protect a web application, commonly hosted on a web server
            - Placed between server and client
        - Used in addition to network-based firewalls
- Implementing a Secure Network
    - Zones, topologies, segmentation, and isolation and various network devices
    - Zones and Topologies
        - Divide network into zones
            - Intranet
            - Extranet

- Boundary protection includes multiple methods to protect the network perimeter
- DMZ
  - Buffer zone
  - Area between firewalls hosting internet facing servers
    - Separating internal network from internet
      - Each firewall uses rules to filter out traffic
- Understanding NAT and PAT
  - NAT translates IPs
    - Public → private
    - Private → public
  - Enabled on internet facing firewalls
    - Commonly used as port address translation
  - Router that connects to internet runs NAT
    - Public IP addresses don't need to be purchased
    - NAT hides internal computer from the internet
  - Not compatible with IPsec
    - IPsec can create VPN tunnels and encrypt traffic with L2TP
  - NAT can be either static or dynamic
    - Static uses a single public IP address in a one-to-one mapping
    - Maps a private IP address with a single public address
    - Dynamic uses multiple public IP addresses in a one-to-many mapping
    - Public IP address is decided based on load

- Network Separation
  - Segregation, segmentation, and isolation
- Physical Isolation and Airgaps
  - Ensures a network isn't connected to any other network
    - Airgaps – red-network (classified)
      - Black network (unclassified)
    - Must be kept absolutely separate
- Logical Separation and Segmentation
  - Routers and firewalls provide a basic level of separation and segmentation
    - Routers segment via ACLs
    - Admins use subnetting
    - Firewalls use packet/content filtering
    - VLANs segment traffic between logical groups of users/computers via logical separation
- Comparing a Layer 2 versus Layer 3 Switch
  - L2 – traditional switch
    - Using MAC address, forwards all broadcast traffic
  - L3 – routers
    - Using destination IP address
    - Block broadcasts
    - L3 switches mimic routers, allow for VLAN creation
      - Uses destination IP address, avoiding ARP-based
- Isolating Traffic with a VLAN
  - Uses a switch to group several different computers into a virtual network
    - Traffic isolated by need
  - Separation based on logical needs (roles) as opposed to physical location
    - Easily reconfigured as needed

- Media Gateway

        - Device that converts data from the format used on one network to the format used on another network
    - Proxy Servers
        - Forward requests for services from clients
            - They can improve performance by caching content and some proxy servers can restrict users access to inappropriate websites by filtering content
        - Located on edge of network
        - Configured by admins for specific protocols
    - Caching Content for Performance
        - Less items that have to be retrieved
        - Reduces bandwidth
    - Transparent Proxy Versus Nontransparent Proxy
        - Transparent – accepts and forwards requests with modification
        - Non-transparent can modify/filter requests
            - Restricts what users can access with URL filters
        - Third-party URL lists can be used as database for go and no-go sites
        - Logs that record site surfing
    - Reverse Proxy
        - Accepts requests from internet for a server
            - Allows server to be located behind second firewall
        - Acts as a load balancer when used with a web farm
    - Application Proxy
        - Accepts requests, forwards, return responds
            - Exchange of data between web services via APIs
    - Unified Threat Management
            - Better security with simplified management
        - UTM security appliances combine the features of multiple security solutions into a single appliance
        - Capabilities include
            - URL filtering
            - DDoS mitigators
            - Malware inspection
            - Content inspection
        - Alerts, output, etc.
        - Common issue → misconfiguration of content filters
        - Commonly placed at network border (but can vary depending on intended use)
    - Mail Gateways
        - Examines all incoming/outgoing email and attempts to reduce risks
            - Between server and internet
            - Can be with UTM
        - Data Loss Prevention (DLP) capability
            - Scan for confidential/sensitive information
            - Blocks it (keyword search)
            - Supports encryption

Chapter 4 – Securing Your Network

- Exploring Advanced Security Devices
- Understanding IDS's and IPS's
        - IDS – monitor networks and send alerts when suspicious events are detected on system or network
        - IPS – react to attacks in progress and prevent them from reaching systems and networks
    - Both capture and analyze traffic with the same monitoring and detection methods

- HIDS
    - Host-based IDS
        - Workstation/server, individual host protection
        - Traffic passes through NICs
        - Can also monitor applications and detect malware traditional AV may miss
- NIDS
    - Network-based IDS
        - Sensors installed on routers and firewalls and report to central monitoring server hosting NIDs console
        - Workstation anomalies cannot be detected unless anomaly affects network traffic
            - Cannot decrypt network traffic
- Sensor and Collector placement
    - Before/after firewall
        - See what exists before and after firewall filter
- Detection Methods
        - Signature based
        - Heuristic/behavioral based (anomaly based)
    - Signature-Based
        - Definition based
        - Database of known vulnerabilities or attack patterns
            - Require constant database updates
    - Heuristic/Behavioral-Based
        - First ID normal operational behavior of a network
            - Performance baseline
        - Compare network behavior against baseline
        - Heuristics takes this a step further
            - Effective at discovering zero-day exploits
        - Baseline should be recreated after every system update
    - Data Sources and Trends
        - IDS uses various raw data sources
            - Firewalls, system app logs provide insight on trends
                - Real-time monitoring
    - Reporting based on rules
        - Configured within IDS and allow reporting of various events
        - Alerts/alarms sent to admins
    - False positives vs false negatives
        - Adjust threshold for happy medium
    - IPS vs IDS
            - Inline vs passive
            - In-band vs out-band
        - IPS can detect, react, prevent
            - Inline – all traffic passes through IPS
        - NIPS placed before DMZ, allowing total inspection, additional NIPS can be installed further in for further filtering against advanced persistent threats (APTs)
- SSL/TLS Accelerators
        - Devices focused on handling TLS traffic
            - HTTPS – certificate + asymmetric encryption
        - Offloading secure connection process to accelerator hardware and offloads resource strain from system CPU and RAM
            - Best placed close as possible to related devices
- SSL Decyptors

    - Attackers use encryption to prevent inspection methods from detecting malware coming into a network
    - Decryptors establish separate TLS session and HTTPS session with malicious site and reads newly decrypted traffic
        - Used in conjunction with NIPS
- SDN
    - Software defined network uses virtualization to route traffic rather than switches/routers
    - Separates data plans and control plans
        - Logic used to forward/block traffic and logic used to identify path to take
    - Allows movement away from proprietary hardware (as hardware uses ACLs)
    - Routers use Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP)
        - SDN uses these protocols without need to create data plan policies to route traffic
            - Plain language
- Honeypots
    - Purposefully vulnerable servers meant to divert attacker's attention away from hard targets
    - Used to gather intelligence on the attackers and observe for potential vulnerabilities or new methods
- Honeynets
    - Group of honeypots within a separate network, accessible from primary network
        - Usually, multiple virtual servers within a single physical server
            - Mimic live network
- IEEE 802.1x Security
    - Port-based authentication protocol that requires users/devices to authenticate when they connect to a specific WAP or physical port (both wired and wireless networks)
        - Blocks access if client cannot authenticate
        - Can be used usernames/pwords or certs and prevents rogue devices
    - Can be combined with VLAN
        - Implemented as Remote Authentication
        - Dial-in user (RADIUS) or Diameter
        - Assists with VPN client authentication
- Securing Wireless Networks
    - Reviewing Wireless Basics
        - Wireless Access Point (WAP)
            - Connects wireless clients to wired network (often with routing capability)
            - All wireless routers are APs
            - Not all APs are wireless routers
        - Switch and Router Components
            - AP's include physical ports for wired access and wireless transceiver
            - Often include NAT, DHCP, etc.
    - Fat versus Thin Access Points
        - Fat AP's – standalone, intelligent, autonomous
            - AP's has everything needed to connect wireless clients to wireless network (router, DHCP, security, ACLs, etc.)
            - Must be configured separate from one another
        - Thin AP's – controller-based – not standalone – wireless controllers configure and manage Thin AP's
            - Allowing for central consolidation
    - Band Selection and Channel Width
        - Two primary bands (2.4 + 5.0 GHz)
        - IEEE 802.11 group of wireless networks
            - 11b → 2.4 GHs → 22 MHz
            - 11g → 2.4 GHz → 20 MHz

        - 11n → 2.4 + 5 GHz → 20 + 40 MHz
        - 11a → 5 GHz → 20, 40, 80, 160 MHz
    - Increased width → more throughput, shorter distance, and greater chance of interference
- Access Point SSID
    - Service Set ID – wireless network name
    - Change default name to enhance security
- Disable SSID Broadcasting or Not?
    - AP's broadcast SSID in cleartext
        - Possible to disable but provides no real clear benefit as attackers can discover SSID w/probe request/response
- Enable MAC Filtering
    - Form of network access control that can be used to restrict access to wireless networks
    - Implicit Deny
        - MACs can be spoofed
- Antenna Types and Placement
    - Omnidirectional
    - Directional
    - Reception is maximized when your AP antenna orientation matches orientation by wireless devices
        - Site surveys assist with planning and repeats maintain environmental picture
- Antenna Power and Signal Strength
    - Lower power → smaller area → restrictive access
- Network Architecture Zones
    - Wireless, guest, ad hoc technologies
- Wireless Cryptographic Protocols
    - WPA
        - Interim replacement for WEP (Vuln)
        - WPA is weak to password cracking
    - WPA2
        - Permanent replacement for WPA
        - Use counter mode with Cipher Blockchaining Message Authentication Code Protocol (CCMP)
    - TKIP versus CCMP
        - Temporal Key Integrity Protocol
            - Used in WPA
            - Deprecated
            - Replaced by AES
        - CCMP
            - WPA2
    - PSK, Enterprise, and Open Modes
        - Pre-shared key mode – wireless access anonymously with PSK/passphrase
            - No authentication, passphrase w/o username provides authorization without authentication
        - Enterprise mode forces users to authenticate with unique credentials before granting access to the wireless network
            - 802.11x server – RADIUS
                - Cert-based authentication
            - Enter in RADIUS server IP, Port, and server password
- Authentication Protocols
        - Built-on EAP (which uses Pairwise Masterkey [PMK])
    - EAP – FAST – Cisco, cert-support

        - Protected EAP (PEAP) – encapsulates EAP convo with TLS tunnel
        - EAP-Tunneled TLS (EAP-TTLS) – extension of PEAP to use PAP
        - EAP-TLS – one of the most secure and widely implemented – req certs on server and clients
        - RADIUS Federation – federation with 802.1x and RADIUS servers
    - Captive Portals
        - Forces clients using web browsers to complete a specific process before allowing network access
            - Free internet access
            - Paid internet access
            - Alternative to IEEE 802.1x
- Understanding Wireless Attacks
        - Most can be avoided using WPA2 with CCMP
    - Disassociation Attacks
        - Removes client from wireless network
        - Disassociation frame is sent to AP with spoofed MAC of victim. AP terminates connection,
            - Victim forced to re-do authentication process
    - WPS and WPS Attacks
        - Susceptible to brute force attacks via PIN attempts
            - REAVER tool
            - Recommend disabling WPS
    - Rogue AP
        - AP placed within a network without official authorization
            - Counterfeit AP's, placed within poorly secured wire-closets
        - Data exfiltration or unauthorized access
    - Evil Twin
        - Rogue AP with same SSID as a legit AP
            - Laptops with wireless access cards
        - Admins use wireless scanners to detect noise and rogue AP's
    - Jamming Attacks
        - DoS by flooding frequency with noise, degrading performance
        - Switch channels or increase AP power
    - IV Attacks
        - Wireless initialization vector attack tries to discover pre-shared key from IV
            - The IV is a number combined with pre-shared key to encrypt data
        - Attacks are successful when IVs are re-used (WEP used 24 number IV)
        - Packet injection increases probability of IV re-use
    - NFC Attacks
        - NFC readers are used to capture data from another NFC device
            - Eavesdropping with antenna-boosted signal
    - Bluetooth Attacks
        - Bluejacking
            - Unsolicited messages sent to nearby BT devices
        - Bluesnarfing
            - Unauthorized access and theft of info from a BT device
                - HCI tool, obexftl
        - Bluebugging
            - Installation of a backdoor via bluesnarfing
        - Rare due to manual acceptance of connection
    - Wireless Replay Attacks
        - Capture and modification of data between two entities to impersonate one of the parties by replaying said data

        - WPA2 using CCMP + AES is not vuln
        - WPA + TKIP is vulnerable
    - RFID Attacks
        - RFID sniffing/eavesdropping – must know frequency and protocols used by RFID system
        - Replay – configure bogus mimic tags
        - DoS – jamming/interference of RFID frequency
    - Misconfigured Access Points
        - AP's not using WPA2 with AES and CCMP
        - WPS being enabled
- Using VPNs for Remote Access
        - Access over a public network
        - Tunneling protocols to encapsulate and encrypt traffic
    - VPNs and VPN Concentrators
        - Direct Access VPN, Routing and Remote Access
            - Two NICs needed
        - Larger organizations use concentrator – dedicated device for VPNs
            - Includes all services for creating VPNs (strong encryption and authentication techniques)
        - Placed in DMZ
            - VPN traffic to concentrator
    - Remote Access VPN
        - Login to VPN client → use RADIUS server for authentication → LDAP server
    - IPsec as a Tunneling Protocol
        - Tunnel and transport modes
            - Tunnel encrypts entire IP packet, used with VPNs (hides internal IP)
        - IPsec provides security via authentication and encryption
        - Authentication Header (AH) encapsulating (ESP) Security Payload protocol #51 and #50, respectively
        - Packet filters use protocol numbers to ID AH/ESP traffic
        - IPsec uses IKE port 500 with security associations (SAS) for the VPN
    - TLS as a Tunneling Protocol
        - Secure Socket Tunneling Protocol (SSTP) encrypts VPN traffic using TLS over port 443
        - Useful for traffic going through a NAT and IPsec is not feasible
            - OpenVPN and OpenConnect
    - Split Tunnel versus Full Tunnel
        - Split Tunnel – Admin determines what traffic should use encrypted tunnel
        - Full Tunnel – all traffic goes through encrypted tunnel and is slower and often used with UTM
    - Site-to-site VPNs
        - Two VPN servers that act as gateways for two networks separated geographically
        - Transparent connection process for end users
    - Always-On VPN
        - Both site-to-site and remote access
- Network Access Control
        - Provide continuous security monitoring by inspecting computers and preventing them from accessing the network
        - Measure of control for computer admins don't have total control over
            - Ensure clients meet pre-determined characteristics
    - Host Health checks
        - Set predefined conditions for healthy hosts
            - Update AV, OS, firewalls

        - Use authentication agents to inspect NAC clients
            - Apps/services that check said conditions
        - Failed clients are directed to a remediation network for quarantine
        - Can also be used for internal client inspection
    - Permanent vs Dissolvable
        - Permanent agents are installed on and stay on a client
            - NAC uses this agent for remote login
        - Dissolvable agents remove themselves after NAC health inspection is done
            - Common on mobiles with BYOD policies
- Identity and Access Services
        - Remote Access Authentication Mechanisms
    - PAP → CHAP
        - PSP used with PPP – cleartext password transmission – rarely used
        - CHAP – PPP with shared secret – hashed with nonce
    - MS-CHAP → MS-CHAPv2
        - Both Microsoft versions of CHAP – mutual authentication
    - RADIUS
        - Centralized authentication service with 802.1x server using WPA2 enterprise
        - Access LDAP server that holds accounts
        - Uses UDP, alternative uses TCP
            - Only encrypts password
            - Alternate encrypt entire process
    - Diameter
        - Extension of RADIUS
        - Can be used with EAP
        - Uses TCP, not UDP
    - TACACS+
        - Cisco alt to RADIUS
        - Encrypts entire authentication process and multiple challenge-response between client and server
        - Can interact with Kerberos
            - Cisco VPN concentrator can interact with Microsoft Active Directory
    - AAA Protocols
        - Provide authentication, authorization, and accounting
            - RADIUS, TACACS+, and Diameter

Chapter 5 – Securing Hosts and Data

- Implementing Secure Systems
    - Secure systems design concepts help ensure that computing systems are deployed and maintained in a secure state
        - Server, workstation, laptop, network device, mobile device
    - Secure systems before deployment and keep secure after
        - Hardening an OS/app by changing from default settings
    - Core principle associated with secure systems design is least functionality
        - Systems deployed only with applications, services, and protocols they need to meet their purpose
            - Accounts, software also
- Operating Systems
    - Different OS's, different versions of OS's
    - Open versus closed source
        - Desktops, laptops, servers, kiosks, networks, appliances
    - Non-persistent operating systems

        - Bootable media
            - Allow an OS to run but disappears once computer is powered down
- Secure Operating Systems Configurations
        - Create master image with a secure configuration, deploy image to multiple systems
        - Trusted OS – meets set of predetermined requirements with heavy emphasis on authorization and authentication
        - Trusted OS's ensure only authorized personnel can access data based on permissions
            - Prevent modification/movement of data
        - Security requirements are often 3rd party – Common Criteria for Information Technology Security Evaluation
            - Mandatory Access Control
    - Using Master Images
            - Streamline secure deployments
        - Start with blank source
            - Install/config OS, apps, security settings
            - Test
        - Capture image
            - Symantec Ghost
            - Stored on external media
        - Deploy
        - Master Images undergo extensive configuration, testing, baseline setting
            - Secure starting point
                - Mandated security configurations
            - Reduced costs
                - Maintenance, reliability
                - Total cost of ownership
            - Virtualization
            - Backups
    - Resiliency and Automation Strategies
        - Automation, scraping, scripting, templates
            - Group policy
            - Microsoft security templates
    - Secure Baseline and Integrity Measurements
        - Starting point
            - Initial configuration
            - Measurements for baseline deviation
                - Automated tools
                    - Vuln scanners, groups
            - Remediation – NAC
    - Patch Management
        - Ensure up-to-date, reducing known vulns
        - ID, download, test, deploy, verify
            - Systems management tools for deployment (SCCM, ConfigMgr)
            - Combined with NAC for automated quarantine
    - Change Management Policy
        - Defines the process for any type of system modifications or upgrades
            - Prevent unintended outages
            - Provide accounting/documentation structure
        - Submit for change approval, logs, for review to return to prefailure state
    - Unauthorized Software and Compliance Violations

        - Susceptibility to fines, penalties, infections, etc.
    - Application Blacklisting and Whitelisting
        - Software restriction policies
            - Microsoft Group Policy
            - Mobile Device Management applications
- Secure Staging and Deployment
    - Sandboxing with VMs
        - Isolated testing areas with high flexibility via virtualization
    - Sandboxing with "Chroot"
        - Linux-based command
        - Changes root dir for an app, isolating it
            - Default is root "/"
                - To create a test environment, copy relevant files to a dir for testing
                - Use chroot to create isolated sandbox chroot jail
                - Any command inputs can only access files within specific dir
                - Files within application can only access other files within test dir path
    - Secure Staging Environment
            - Multiple environments with different systems per stage
        - Development – version control and change management
        - Test – test modules for flaws/bugs
        - Staging – simulated production environment
            - Complete but independent copy
        - Production – final product
- Peripherals
    - Wireless keyboards, mice – can be intercepted
    - Displays – limit over the shoulder view
        - Privacy screens
    - External Storage Devices
        - Prevent or limit use, control use to prevent misuse, abuse, loss
    - Cameras
    - Wi-Fi MicroSDs – interception of transmissions
        - Strong wireless security needed
    - Printers/Multifunction Devices
        - Extra features
        - Embedded systems
        - Storage
- Hardware and Firmware Security
        - Consider supply chain, reputable source
    - EMI and EMP
        - Electrostatic discharge, lightning, military weapons
    - Full-Disk Encryption and Self-Encrypting Devices
        - VeraCrypt, hardware and software
    - UEFI and BIOS
    - Trusted Platform Module
        - Hardware chip on motherboard, stores crypto keys
        - Keep hard drives sealed while system completes a system verification and authentication process
        - Secure boot and attestation
            - Key files are signatured and stored upon configuration
                - Secure boot check files against signs to ensure integrity
            - Remote attestation checks boot files via separate system

        - TPM uses RSA-burned in key for asymmetric encryption
            - Hardware root of trust
            - Microsoft Bitlocker
                - Platform verification with authentication process
    - Hardware Security Module
        - Add to a system to manage, generate, and securely store crypto keys
        - Can be external devices connected via TCP/IP or expansion cards, or port-connected
    - Additional Vulnerabilities
        - End-of-life systems, lack of vendor support
- Summarizing Cloud Concepts
        - Software as a service, cloud computing
        - OneDrive, google drive, cloud, EC2
        - On-premises or hosted (cloud) services
    - Software as a Service (SaaS)
        - Network
        - Web browser
    - Platform as a Service
        - Preconfigured computing platform to be used as needed
            - On demand, easy to use
        - Managed hardware
            - Users manage software
    - Infrastructure as a Service
        - Outsource equipment requirements, customer rents access
            - Self-managed
            - Customers configure server past default
    - Security Responsibilities with Cloud Models
        - CSP vs Customer
            - SaaS – CSP (75%)
            - PaaS – CSP (50%)
            - IaaS – CSP (25%)
    - Security as a Service
        - Subset of SaaS
            - AV
        - Outsources admin tasks associated with implementing service
            - Allows specialized focus
        - Cloud access security broker (CASB)
            - Tool, device, service deployed between organization network and CSP
    - Cloud Deployment Models
        - Public, private
        - Community, hybrids
- Deploying Mobile Devices Securely
        - NIST SP800-124
    - Deployment Models
        - Any connected device is a risk
            - Must monitor and manager
                - Especially beyond BYOD
            - Corporate owned
            - Corporate owned, personally enable
            - BYOD
            - Virtual Desktop Infrastructure

- Connection Methods
  - Cellular, SATCOM, NFC, IR, WiFi, Bluetooth, ANTC(+), USB
- Mobile Device Management
  - Expansion of SCCM to mobile
  - App Management
  - Full Device Encryption
  - Storage Segmentation
  - Content Management
  - Containerization
  - Passwords + PINs
  - Biometrics
  - Screen Locks
  - Remote Wipe
  - Geolocation
  - Geofencing, Geotagging
  - Context-Aware Authentication
  - Push Notification Services
- Mobile Device Enforcement and Monitoring
  - Compliance, block access
    - NAC
- Unauthorized Software
    - Third party app store
    - Jailbreaking, rooting
    - Custom firmware
    - Sideloading
  - MMS + SMS are plaintext
    - iMessage (encrypted)
  - MMS messages can allow remote code execution
  - Payment info, PII, etc. stored
- Hardware Control
  - Camera, mic in phone
    - MDM disabling with geofencing
  - Prevent USB on the go cables
- Unauthorized Connections
  - Limit simultaneous connections (phones connection internally, externally)
    - Tethering, hotspots
  - Bypasses content filters
  - Wi-Fi Direct (ad hoc)
    - Uses single hop radio
    - Carrier unlocking

- Exploring Embedded Systems
  - Dedicated function device that uses a computer system to perform said function
- Security Implications and Vulnerabilities
  - Must keep embedded systems up to date
    - Default configs
  - Comparing embedded systems
    - Smart TVs, IoTs
    - Wearable tech, implantable
    - Home automation
    - System on a chip, ICS, SCADA (NIPS, NACS, VLANS)
    - HVAC

        - Real-time OS
            - Reacts to input within a specific time (assembly line)
        - Medical, automotive, UAVs
    - Protecting Data
        - Security contracts an organization can use to protect data based on the requirements set within a data security policy
        - Encryption and strong access controls
- Protecting Confidentiality with Encryption
        - Data both at rest and transit
    - Database Security
        - Encrypt database elements
    - File System Security
        - Linux
            - GNU Privacy Guard (command line tool)
        - Windows → Encrypting File System
        - Individual file encryption
    - Permission Issues and Access Violations
        - Principle of least privilege to prevent access violations
    - Linux Permissions
        - Owner, group, others
            - Permissions – Total = 5, 6, 7
                - Read - 4
                - Write - 2
                - Execute – 1
            - Chmod command to change file permissions
    - Windows permissions
        - Read, write, read and execute, modify (delete or r w ex)
- Data Loss Prevention
    - Removeable Media
        - Prohibit use, technical policies block use
        - DLP solution – selective – block copy/print specific content
            - Also log events, alert admins
    - Data Exfiltration
        - UTM devices – incoming
        - DLP devices – outgoing
            - Scan for PII and other sensitive data, even encrypted or zipped
            - Block leakage
    - Cloud-based DLP
        - PII, PHI – alerts, blockage, logs, etc.
            - Quarantine

Chapter Six – Comparing Threats, Vulnerabilities, and Common Attacks

- Understanding Threat Actors
        - Gathering open-source intelligence
        - Script-kiddies, hacktivists, insiders, organized crime
        - State/nation-sponsored can launch advanced persistent threats (APTs) against networks
            - GRIZZLY STEPPE
            - DoS/DDoS
                - Overload NIC traffic
                - Resource exhaustion
- Determining Malware Types
    - Viruses

        - Attaches to host for replication and execution
    - Worms
        - Self-replicating virus, residing in memory without host or application interaction
        - Consumes bandwidth
    - Logic Bombs
        - Code that executes as event response
    - Backdoors
        - Effective network access policies must be used to mitigate backdoor creation
    - Trojans
        - Attacks often compromise websites
        - Install embedded trojans
        - Trick users to visit compromised site
        - Website attempts trojan download
        - Rogueware, scareware, fake AV
    - Remote Access Trojans (RATs)
        - Delivered via drive-by downloads
        - Keyloggers, credential stealers
    - Ransomware
        - Drive-bys, embedded downloads
        - Crypto-malware, doxing
    - Keyloggers
        - Software or hardware-based
    - Spyware
        - Monitor user activity
        - Privacy-invasive, data-harvesting
        - Impersonation, ID theft
    - Adware
        - Consumer info-gathering, targeted Ads
        - Web and behavioral analytics
    - Bots and Botnets
        - Software robots, zombies
            - Bot herders with command and control (C2) servers
                - Mirai
        - IoTs
        - Spam, DDoS, additional malware downloads commands
    - Rootkits
        - Modify internal OS, hidden from common AV
        - Modify Registry, system-level access
            - Root/kernel, intercept calls to OS via hooking
        - Hooking may be detectable by AV examining RAM contents
- Recognizing Common Attacks
    - Social Engineering
            - low-tech social tactics to gain info
            - flattery, impersonation, pressure
            - ask direct or roundabout but relevant questions
        - Impersonation
            - ID verification methods
        - Shoulder Surfing
            - Counter with positioning or filters
        - Hoaxes
        - Tailgating and Mantraps

        - Counter tailgating with mantraps
    - Dumpster Diving
        - Shred/burn sensitive material
            - Anything with PII/PHI
    - Watering Hole Attacks
        - Discover what websites a group of people visit and attempt to compromise that site with malware
- Attacks via Email and Phone
    - Spam
        - Unwanted/unsolicited email
    - Phishing
    - Emails from "Friends"
        - Impersonation
    - Phishing to Install Malware
        - Pique curiosity
    - Phishing to Validate Email Addresses
        - Use beacons to validate email addresses for image viewing
            - Disabled by default
    - Phishing to Get Money
    - Spear Phishing
        - Targeted form
            - Counter with digital signatures for impersonation
    - Whaling
        - High-level targets of spear Phishing
    - Vishing
        - Use of phone, VoIP via spoofed caller ID
- One Click Lets Them In
        - APTs need a single click
        - Attacker space → neutral space → victim space
    - Open source intelligence
    - Phishing creation
    - Phishing deployment
    - User activates phishing attempt
    - Malware download
    - Attacker accesses targeted systems
        - Network vulns
    - Malware Spread
    - Internal data collection
    - Internal data packaging
    - Internal data exfiltration
    - Privilege escalation
- Blocking Malware and Other Attacks
    - Protecting Systems from Malware
            - Implement layered defense-in-depth
        - Spam filter on mail gateways
        - Anti-malware software on mail gateways
        - All systems
        - Boundaries and firewalls
            - UTM
    - Antivirus and Anti-malware Software
            - Regular scans, manual + automatic

        - Recognize and react to alerts
    - Signature-based
        - Signature files compared with database
        - Make sure database is constantly updated
            - Compare hash for integrity
    - Heuristic-based detection
        - Use sandboxes and VMs to test unknown code
        - Compare with baseline behavior
            - Good for polymorphic detection
    - Checking file integrity
        - Hashes for baseline
            - Detects rootkits
        - Command line – Microsoft file checksum integrity verifier (fciv.exe)
        - Any detected modified exes are likely malware
    - Data execution prevention
        - Prevents code from executing in memory regions marked as non-executable
        - Hardware and software enforcement
            - AMD – NX
            - Intel – XD
            - Windows – SysProp – Performance Settings
    - Advanced Malware Tools
        - Analyze network with threat intelligence and analytics
            - Continuous analysis
            - Analysist view logs and alerts
    - Spam Filters
        - UTMs
        - Spam and junk filters
            - Rely on email ID white/blacklist
- Educating Users
    - Awareness and training
    - Understand risks and methods
    - Recognize and respond
  - New viruses
    - Patch and update
    - Evaluate, test, implement
  - Phishing attacks
    - Prevented with education
  - Zero-day exploits
    - Cover gaps AV cannot account for
        - Safe computing practices
            - Careful with links
                - Attachments
                - Downloads
        - Limit public info
        - Backup data, up to date patches, and AV
- Why Social Engineering Works
  - Psychology
    - Authority
        - Impersonation, phishing, vishing, whaling
    - Intimidation

        - Trust
        - Consensus
        - Scarcity
        - Urgency
        - Familiarity + shoulder surfing/tailgating

Chapter 7 – Protecting Against Advanced Attacks

- Comparing Common Attacks
    - Dos vs DDoS
        - one vs many
        - DDoS sustained high traffic attacks on NICs, RAM, CPUs
    - Privilege Escalation
        - various privilege escalation techniques
    - Spoofing
        - MAC address spoofing – software
            - Flood Guards can prevent MAC spoofing
        - IP address spoofing
    - SYN Flood Attack
        - common against servers on the internet
            - easy to launch, hard to stop by disrupting TCP handshake process
        - threshold for connections or memory max is reached
            - Linux IP tables allows for SYN packets
    - Man in the Middle Attacks
        - active interception/eavesdropping with victims unaware of MitM
        - Kerberos prevents this with mutual authentication
        - can also be launched via ARP poisoning
    - ARP Poisoning
        - misleads computers, switches about actual MAC address of a system
        - ARP resolves IP addresses to MAC addresses with ARP requests and replys
            - ARP is very trusting, believing any ARP reply
        - spoofed ARPs can be created, poisoning a systems ARP cache
    - ARP MitM Attacks
        - a poisoned ARP cache will redirect traffic to a malicious site/user
        - used with IP forwarding to send the traffic to the router so victim remains unaware
    - ARP DOS Attacks
        - attacker sends ARP reply with bogus default gateway MAC address
        - if computers cache bogus DG MAC Address, no traffic will leave network
    - DNS Attacks
        - some applications use reverse lookup as a rudimentary spoofing detector
            - useful when available but optional on DNS servers – not always available
        - DNS Poisoning Attacks
            - modify/corrupt DNS results
            - prevented with DNSSEC
        - Pharming Attacks
            - corrupt DNS server/client, redirecting user
                - client computers have their hosts file modified so user traffic is directed to a malicious site
        - DDoS DNS Attacks
            - Mirai software used to attack DNS server performance companies
    - Amplification Attacks
        - form of DDoS that significantly increases the amount of traffic sent to/requested from a victim

        - commands tell computers/servers to reply with as much data as possible to victims IP
            - overloads system
    - NTP server with manlist cmd, for example, floods specified IP with data about 600 systems
- Password Attacks
    - Bruteforce Attacks
        - online/offline
            - account lockout countermeasure
            - limit login wait time or attempts per second
            - store complex passwords with encryption or hashed
    - Dictionary Attacks
        - use complex pwrds
    - Password Hashes
        - hash attacks use free tools to reverse a given hash, if the hash algorithm is known
        - hash password still requires encryption before being sent along network
        - crackstation, hydra, hashcat
    - Pass the Hash Attack
        - discover hash and used for authentication
            - common with Microsoft LAN manager and NT LAN manager
                - doesn't encrypt hash traffic
            - use NTLMv2 or Kerberos instead
                - NTLMv2 uses nonce and challenge/response
        - configure clients to only send NTLMv2 responses and configure authenticating servers to refuse any use of LM or NTLM
            - done via Group Policy
    - Birthday Attacks
        - birthday paradox
            - use a password that can produce same hash as another password
        - hash collision
        - countered by increasing number of bits used in the hash
    - Rainbow Table Attacks
        - discover password from hash
        - rainbow tables are huge databases of pre-computated hashes
            - application compares hashes until a match is found
        - countered with salting passwords
            - salt – random data set, such as two additional characters to a password before the hash
- Replay Attacks
    - attack replays already sent data, impersonating a client
    - thwarted with timestamps and sequence numbers
- Known Plaintext Attacks
    - samples of both plaintext and ciphertext to discover encryption/decryption methods
    - chosen plaintext is a sample, but no access to all plaintext
        - like an end statement that is always repeated
    - known and chosen will be successful with sufficient time and resources
        - cipher – only is successful with weak encryption keys
- Hijacking and Related Attacks
    - type squatting and URL hijacking
        - buying domain close to another in name
    - host malicious sites, earn ad revenue, resell domain

        - clickjacking
            - countered with breaking or disabling frames so attackers cannot display a webpage within a frame on another site
        - session hijacking
            - session IDs in cookies used for impersonating a victim
    - Domain Hijacking
        - changes registration of a domain name without permission
            - common with social engineering
    - Main-in-the-Browser
        - proxy Trojan horse that can capture browser session data (keylogging)
            - ex. Zeus
    - Driver Manipulation
        - driver shimming allows older drivers to be compatible with newer operating systems
            - refactoring is a total rework
        - programmers can write shims or refactors to fool OS into using a manipulated driver
    - Zero-Day Attacks
    - Memory Buffer Vulnerabilities
            - use secure memory management techniques within code to counter
        - Memory Leak
            - bug in app that causes app to use more and more memory the longer it runs
                - potentially crashing OS
            - typically caused by apps that reverse but never release memory intended for short term use
        - Integer Overflow
            - use/create a number too big for an application to handle
                - results in inaccuracies
            - double check buffer size
        - Buffer Overflow and Buffer Overflow Attacks
            - app receives more/different input than it expects, exposing normally protected system memory
                - expanding application memory access beyond pre-allocated buffers
                    - giving attacker opportunity to write malicious code in this new area of memory
                - can be used for DoS
                - typically used for code insertion that victim system will execute
            - error handing and input validation can counter most instances
                - maintain patches
        - Pointer Deference
            - passing references to a data array (common in C, C++, Pascal, Java)
            - Deference is the process of using the pointer to access the data array
                - failed deferences can crash an application or corrupt data
                - caused by pointing to nonexistent points
        - DLL Injection
            - Dynamic Link Libraries
            - DLL Injection injects a DLL into system memory and runs it
- Summarizing Secure Coding Concepts
    - Compiled versus Runtime Code
        - Compiled – optimized into an exe
        - Runtime – evaluated, interpreted, and executed when code is run
        - Hybrid
    - Proper Input Validation

        - check data for validity before using it
            - sanitize/reject input
        - improper validation allows for buffer overflow, SQL Injection, XSS, Command Injection
        - Verify proper characters, boundary/range checks, block HTML code, character-use limits
    - Client-side and Server-Side Input Validation
        - browser versus server
    - Other Input Validation Techniques
        - sanitize HTML, escaping/encoding HTML
            - OWASP ESAPI can be used
- Avoiding Race Conditions
    - two or more modules/applications attempt to access a resource at the same time
        - methods available to avoid
        - internal concurrency controls
- Proper Error Handling
    - catch and gracefully handle errors and prevent crashes
        - errors presented to users should be vague
        - detail information should be logged internally
- Cryptographic Techniques
    - encrypt sensitive data at rest/transit
    - certificate use
    - code signing and hashing of code
- Code Reuse and SDK
    - avoid dead code via copy/paste or logic errors, third party libraries
        - SDKs are single party libraries
- Code Obfuscation
    - make code unreadable
    - tenable solution, not widely accepted
- Code Quality and Testing
    - static code analyzers
    - dynamic analysis
    - stress testing
    - sandboxing
    - model verification
- Development Life cycle Models
    - Waterfall – top to bottom in stages
    - Agile – cross-functional teams
- Secure DevOps
    - communication between developers and operations personnel
    - security considered throughout the process
        - security automation
        - continuous integration
        - baselining
        - immutable systems
        - infrastructure as lode
- Version Control and Change Management
    - ensure development control, overlapping oversight
    - track software updates with versioning
        - rollbacks
- Provisioning and Deprovisioning

        - user accounts, applications, etc
- Identifying Application Attacks
        - web servers → buffer overflow, SQL Injection, cmd injection
    - Web Servers
        - apache
        - Internet Information Services
    - Database Concepts
        - SQL, tables, fields, columns/rows
    - Normalization
            - organizing a database to reduce redundancy, increase performance
        - First Normal Form
            - each row unique and Id'd with primary key
            - related data is contained on a separate table
            - no columns have repeating groups
        - Second Normal Form
                - composite primary key required (two + columns)
            - INF
            - Non-primary key attributes are completely dependent on composite primary key
        - Third Normal Form
                - eliminate redundancy
            - INF + 2NF
            - all columns not primary key are only dependent on primary key
    - SQL Queries
            - injection attack vulnerabilities as SQL queries format results of a database into a web page
        - SQL Injection Attacks
            - entering of additional data into web page form to generate different SQL statements
                - vulnerable without error-handling routines
            - begins with improperly formatted SQL statements to system to generate errors
                - limiting error response details is essential
        - Protecting Against SQL Injection Attacks
            - input validation
            - stored procedures (SQL mini programs that exe as a whole)
                - user input stored as a parameter
                    - perform validation, prevents SQL injection
    - Injection Attacks
        - command injection, OS commands
            - directory traversal via input box
    - Cross-Site Scripting
        - XSS
            - embedded HTML/JS
        - counter with input validation
        - security encoding
    - Cross-Site Request Forgery – CSRF
        - attacker tricks user into performing an action on a webpage
            - via HTML link
            - if a website supports any action via an HTML link
                - post-login stored in cookies can be a gateway by accessing login info
            - developers must be aware of CSRF

        - dual authentication
        - expire cookies
        - XSRF tokens
- Understanding Frameworks and Guidelines
    - best practices and instructions
        - regulatory – HIPPA
        - non-regulatory – COBIT
        - national versus international – NIST vs ISO, IEC
        - industry-specific – PCI DSS
    - benchmarks, configuration standards, guidelines
        - OS-based, role-based

---

Chapter 8 – Using Risk Management Tools

- Understanding Risk Management
        - risk/vulnerability/threat matrix
        - result/impact
        - risk management balanced with utility of protected system
    - Threat and Threat Assessments
        - Compromise Cia Triad
            - malicious humans
            - accidental human action
            - environmental
        - Assessment
            - threat and risk prediction, potential resource balance
            - ID prevention measures
            - environmental, manmade, internal, external
    - Vulnerabilities
        - lack of updates, default configs, lack of present/good AV/M, lack of firewalls, lack of or bad organizational policy
    - Risk Management
        - ID – Monitor – Limit Risks
            - Reduce to organizationally acceptable level
        - Risk Response Techniques
            - avoid – don't use/offer services/products
            - transfer – transfer risk via insurance or third party services
            - mitigate – reduce vulns or impact potential
            - accept – cost-benefit analysis of risk vs impact vs outcome
        - Risk Assessment
            - qualify vs quantify
                - ID assets and values
                - ID threats via vulns to each asset
                - ID recommendations
            - snapshot assessment
    - Quantitative Risk Assessment
            - asserts monetary value to risks, impacts, assets
                - revenue, replacement cost
            - Single Loss Expectancy (SLE) = ALE/ARO
            - Annual Rate of Occurrence (ARO) = ALE/SLE
            - Annual Loss Expectancy (ALE) = SLE(ARO)
        - cost vs savings of a given action

- Qualitative Risk Assessment
  - judgement to build and assign categorized risks on likelihood and impact
  - use surveys, focus groups
  - low, medium, high
- Documenting the Assessment
  - Review risks, assessments, recommendations
    - influence implementation/acceptance of decision
  - Risk Registers
    - Projects IN Controlled Environments (PRINCE2)
    - Personalized data tables with categories, specified risks, likelihoods, impacts, scoring, control/mitigation, contingencies, action assignment and deadline
  - Supply Chain Assessment
    - all processes required to create and distribute a finished product from raw materials
    - evaluate such elements
      - ID single points of failure, redundancies

- Comparing Scanning and Testing Tools
  - Checking for Vulnerabilities
    - vulnerability assessments and network vulnerability scans to assess security posture
    - include info from policies, logs, interviews, and system tests
      - scans and pentests to ID assets and capability → assign value/priority → ID vulns and prioritize → recommend controls and mitigations
  - Password Crackers
    - offline and online, used in pentests to test for encryption/hash strength or plaintext possession
  - Network Scanners
    - nmap, netcast, nessus
    - ping, ARP ping, Syn Stealth
    - port scan, service scan, OS detection
  - Network Mapping
    - focus on connectivity – zenmap
  - Wireless Scanners and Crackers
    - site surveys, passive and active
      - SSIDs, MACs, Signal Strength, Channels + widths, security
  - Rogue System Detection
    - known vs unknown SSIDs
      - received signal strength indicator
    - Banner Grabbing
      - gain information about remote systems, ID OS and applications with HTML banner
        - Netcat
    - Vulnerability Scanning
      - ID vulns, misconfigs, passively test security controls
  - Identifying Vulnerabilities and Misconfigurations
    - using database, dictionary
      - CVE, SCAP (NVD)
        - open ports, weak passwords, default accounts and passwords, sensitive data, security and configurations error
  - Passive Testing of Security Controls
    - ID – not exploit

    - ID Lack of Security Controls
        - lack of patches or AV
    - False Positives
        - Credentialed versus non-Credentialed
            - attacks typically run non-credentialed scans
            - security admins run with privileged credentials for deeper scans
            - attackers will gain credentialed access
        - Configuration Compliance Scanner
            - verify system configs, validation and usually automated via scripting
- Obtaining Authorization
    - written consent, rules of engagement to ID boundaries
- Penetration Testing
            - active assessment of deployed security controls to determine threat impact
            - also test penetration response → weakness in policy and business continuity
        - Passive Recon → Active Recon → Initial Exploit → Escalate Privilege → Pivot → Persistence
        - Passive – OSI
        - Active – net scanners
        - Initial – ID vulnerable applications
        - Escalation
        - Pivot – network spread
        - Persistence – backdoors, ssh
    - White, Gray, Black Box testing
- Intrusive Versus Non-Intrusive Testing
        - scans can be either, pentesting being intrusive and vuln scanning being non-intrusive
- Passive versus Active Tools
    - cannot directly versus directly affect system operations
- Exploitation Frameworks
        - tools for vuln checking and executing exploits
            - Metasploit framework
            - browser exploitation framework
            - web application attack and audit framework
- Using Security Tools
    - Sniffing with a Protocol Analyzer
            - IP headers and packets with sniffers connected via rogue switch
            - wireshark
        - manipulate flags within headers for attackers
            - verify header manipulation attacks
        - quantify traffic
        - must set NIC to promiscuous mode to interpret all packets received
    - Command Line Tools
        - TCPdump
        - Nmap
        - Netcat
            - banner grabbing, transferring files, port scanner
        - Monitoring Logs for Event Anomalies
            - ID what happened, when
            - Event anomalies
            - logging limited by space
    - Operating Systems Event Logs

        - basic logs, Windows Event Viewer, Security Log
        - Auditing
            - Application Log
            - System Log
    - Firewall and Router Access Logs
        - troubleshoot connectivity, ID'ing potential intrusions/attacks
    - Linux Logs
        - system log viewer
            - cat /var/log/auth.log
                - messages, boot.log, auth.log, failog, kern.log, httpd/
        - other logs
            - AV, apps, Performance
- SIEM
        - Security Information and Event Management Systems
        - Centralize → collecting, analyzing, managing data
            - combine real-time SEM and long-term storage of SIM
        - NOC
    - Capabilities
        - Aggregation
        - Correlation Engine
        - Automated Alerting
        - Automated Triggers
        - Time Synch
        - Event Duplication
        - Logs/WORM
    - Located within private network
- Continuous Monitoring
        - emerging threats, new vulns
        - monitor security controls, maintain security posture
            - threat assessments
            - vuln assessments
            - risk assessments
        - scans, pentests, audits, reviews
- Usage of Auditing and Reviews
    - logging information on what users do
        - login attempts
    - usage auditing review
        - audit trial
- Permission Auditing and Review
        - rights and permissions assigned to users and help ensure least privilege
        - detect privilege creep/permission bloat
        - account management practices

---

Chapter 9 – Implementing Controls to Protect Assets

- Implementing Defense in Depth
        - layered security
        - control diversity
            - combo of technical, administrative, physical controls
            - IDS, proxy servers, firewalls, assessment and testing
        - vendor diversity
            - security controls from various vendors

        - two firewall DMZ using two vendors
    - user training
- Comparing Physical Security Controls
    - perimeter, buildings
    - secure work areas, server and network rooms
    - hardware airgap
    - use signs
    - mixed door types
        - limit entry
        - cipher locks
            - don't ID users
            - shoulder surfing
        - proximity cards, smart cards, tokens
            - combine with PIN
    - Biometrics
  - Tailgating
    - authorized users doing this equates to a socially engineerable environment
    - counter with guards, education, traffic flow measures
  - Preventing Tailgating with Mantraps
    - turnstiles, airlocks
  - Increase Physical Security with Guards
  - Monitor Areas with Cameras
    - CCTV
    - public areas, employee awareness, no audio
  - Fencing, Lighting, Alarms
    - gates, automated lights, fire alarms, unauthorized access
    - infrared, motion
  - Securing Access with Barricades
    - zigzag for vehicles
    - bollards
  - Hardware Locks
    - Secure Mobile Computers with Cable Locks
    - Secure Servers with Locking Cabinets
    - Secure Small Devices with Safe
  - Asset Management
    - process of tracking valuable assets throughout their life cycles
        - reduce architecture and design weaknesses
            - purchases going through an approval process
    - system sprawl and undocumented assets
        - underutilized assets due to more possessed than needed
    - inventory control
        - RFIDs
  - Implementing Environmental Controls
    - HVAC – avoid drastic temperature changes
    - Hot and cold Aisles
        - alternate so hot air wont be intake for next row of racks
    - fire alarms integrated so 02 wont be fed to fire if detected
        - dampeners
    - Fire suppressors
        - individual or fixed systems
        - remove heat, 02, fuel, disrupt chain reaction

        - alternate power during failures
        - environmental monitoring
            - temp, humidity, logging
    - Shielding
        - limit EMI and RFI
            - prevent attacker from capturing network traffic
        - protective cabling
            - UTP (Cat5e and Cat6)
                - shielded TP (STP) and Unshielded TP (UTP)
            - fiber cables do not create interceptible induction fields
        - protected distribution of cabling
            - planning where and how cables are routed → physical security
            - Faraday Cages
                - prevent signal transmission
- Adding Redundancy and Fault Tolerance
        - increase reliability in the face of failure through redundancy
            - provides fault tolerance by eliminating single point of failure
        - multiple Levels
            - Disk vs RAID
            - Server via failover clusters
            - power via generators/UPSs
            - site via hot, cold, warm sites
    - Disk Redundancies
        - RAID 0 – striping, no redundancy
        - RAID 1 – mirroring, removes SPoF
        - RAID 10 – combine striping and mirroring
            - requires a minimum of four drives and increases in increments of two
    - Server Redundancy and High Availability
        - remain operational without downtime – 99.999% achievable via redundancy and fault tolerance
            - expensive
            - distributive allocation is also used
        - Failover Clusters for high availability
            - two+ servers clustered that take over load of failed nodes
        - Load Balancers for High Availability
            - instead of passive/active nodes, all nodes share load
            - optimized/distributable data loads, localized in DMZ
                - software or hardware
            - provides scalability, round robin structure
            - detect when a server fails
        - Clustering versus Load Balancing
            - weigh pros and cons
    - Power Redundancies
        - UPS, Generators
- Protecting Data with Backups
        - important to maintain the existence of a useable backup
    - Comparing Backup Types
        - full backup – time + money
        - different backup – full backup + further changes (reduces backup time)

        - incremental backup – full + incremental changes (requires two backups, OG + differential)
        - Snapshots – VMs and checkpoints
    - Testing Backups
        - perform test restore
            - ensure practice and status of backup integrity
        - protect in storage, transfer, and ensure destruction when no longer needed
        - create backup policy
            - consider
                - off-site backups
                - distance
                - location selection
                - legal implications
                - data sovereignty
                    - relevant to where data is stored and the laws of that locale
- Comparing Business Continuity Elements
    - predict and plan for potential outages
    - Business Continuity Plain
    - Business Impact Analysis Concepts
        - critical part of BCP
        - ID critical assets, mission essentials
            - quick restore
        - must be completed in advance
            - what are critical systems/functions
            - what dependencies do they have
            - what is max downtime
            - what scenarios are most likely to impact
            - what is potential loss of said scenarios
    - Impact
        - life, property, safety, financial loss, reputation
    - Privacy Impact and Threshold Assessments
        - NIST SP 800-122
            - ID PIIs
                - conduct privacy impact assessment
    - Recovery Time Objective
        - max time to restore system post outage
            - varies by asset
    - Recovery Point Objective
        - point of time were data loss is acceptable
    - Comparing MTBF and MTTR
        - Mean Time Between Failures
            - provides insight to system reliability
        - Mean Time To Recover
            - specifically mentioned in maintenance contracts
    - Continuity of Operations Planning
        - restoring mission essential functions at a recovery site
    - Recovery Sites
        - hot
            - 2-4 hours
            - $$$
        - warm

        - $$
    - cold
        - $
        - longest options
    - mobile and mirrored options are also available
- Order of Operation
    - least critical first

- Disaster Recovery
    - address systems hosting critical systems and components
    - can have multiple DRPs in a BCP
        - hierarchy of critical systems
- Activate the DRP
    - implement contingencies
        - recover critical systems
            - test recovered systems
                - After-Action Report

- Testing Plans with Exercises
- NIST SP 800-34
    - Table Tops
    - functional exercises
- test backups, server restoration, server redundancy, alternate sites

---

Chapter 10 – Understanding Cryptography and PKI

- Introducing Cryptography Concepts
    - core concepts – integrity and confidentiality
        - integrity – hashes
        - confidentiality – encryption (symmetric, asymmetric [PKI])
            - stream and block ciphers
            - steganography
            - digital signatures
                - authentication
                - non-repudiation
                - integrity
- Providing Integrity with Hashing
        - hash/checksum of fixed length
            - create two for comparison
        - MD5 – 128bit hash – 32 hex characters – vulnerable
        - SHA0-3
            - 1 – 160bit
            - 2 – 256, 512, 224, 384
            - 3 – 224, 256, 384, 512
        - HIDs compare hashes against a database
    - HMAC
            - Hash-based Message Authentication Code with shared secret key to add randomness
            - integrity and authenticity
            - IPSec and TLS use HMAC-MD5/SHA1
    - RIPEMD – Race integrity Primitives Evaluation Message Digest
        - 160, 128, 256, 320 bits
    - Hashing Files

        - typically automated, can be manual
    - Hashing Passwords
        - compared automatically between database and user input
    - Key Stretching
        - salt passwords
            - bcrypt and password-based key derivation function 2 (PBKDF2)
        - bcrypt – blowfish block cipher
            - unix/linux – shadow file
            - 60 character string
        - PBKDF2 – 64 bits and HMAC
            - WPA2, IoS, Cisco = 128, 256, 512
            - replaced by Argon2
    - Hashing Messages
        - comparison for integrity checks
    - Using HMAC
        - helps prevent hash modification as attacker does not know secret key
- Providing Confidentiality with Encryption
        - also prevents unauthorized disclosure
        - protects data at rest, transit, and use
        - algorithm + key
    - Encryption Terms
        - random + pseudo – random numbers
        - initialization vector – IV – starting value
        - nonce – number used once
        - XOR – logical operation used in encryption with Boolean return
        - Confusion – cipher and plaintext are extremely different
        - Diffusion – small plaintext changes result in large changes in the ciphertext
        - Secret Algorithm – (a now discouraged practice)
        - Weak/Deprecated Algorithms – like SSL
        - High Resiliency – encryption key remains secure even if part of key is discovered
    - Block versus Stream Ciphers
            - block – 64/128 bit
                - better with known data sizes
            - stream – 1 bit at a time
                - better with unknown data sizes
    - Cipher Modes
        - Electronic Codebook (ECB) – plaintext blocks encrypted with same key
        - Cipher Block Chaining (CBC) - symmetric block ciphers
            - uses IV, combining subsequent blocks with XOR
                - pipeline delays
        - Galois/Counter Mode – block ciphers
            - counter + Galois authentication for data
            - widely used
    - Symmetric Encryption
        - substitutional, ROT13
            - obfuscation
        - AES – 128, 256; RADIUS
            - constant key change to heighten security
            - block cipher – NIST – fast, efficient, strong
                - keys – 128, 192, 256
        - DES – 64 bit blocks, 56 bit key

- 3DES – 3 passes of DES with multiple keys – 64 bit blocks
    - keys – 56, 112, 168
        - less common than AES
- RC4 – symmetric stream cipher – 40-2048 bits
    - used with SSL, TLS, HTTPS
        - potentially broken
            - AES with TLS recommended
- Blowfish and Twofish
    - Blowfish – symmetric block cipher – 64 bit blocks – keys 32-448 – faster than AES-256
    - Twofish – 128 blocks – keys 128, 192, 256

- Asymmetric Encryption
    - public and private keys
    - resource intensive
        - used for key exchange
        - digital signature, encryption
- Certificates
    - include public key and info about owner of certificate
        - issued and managed by Cas
            - serial # , validity dates, usage
            - issuer, subject, public key
- RSA
    - very commonly used
        - uses prime numbers, product of two large primes
        - 2048 bits – secure to 2030
        - 3027 bits – secure beyond 2030
- Static versus Ephemeral Keys
    - Static – semi-permanent – RSA – Certificate Lifetime
    - Ephemeral – recreated per session – some versions of Diffier-Hellman – perfect forward secrecy
        - a cryptosystem generates random public keys per session without deterministic algorithm
            - avoid reusing keys
- Elliptic Curve Cryptography
    - less resource intensive
        - low power devices
            - deprecated since 2015
- Diffie-Hellman
    - key exchange algorithm
    - static or ephemeral
        - ECDH, DHE, ECDHE
    - two parties negotiate strongest group supportable by both parties
        - 25 groups
- Steganography
    - manipulating bits
        - hide data in file whitespace
- Using Cryptographic Protocols
    - email digital signatures
        - sender private = E
        - sender public = D
    - email Encryption

        - recipient – public – E, private – D
    - Website Encryption
        - web site public – E, private – D
            - symmetric key – E for session
- Protecting Email
    - Signing Email with Digital Signatures
        - DSA – Digital Signature Algorithm
            - message → hash → encrypted with senders private key
        - authentication, non-repudiation, integrity
    - Encrypting Email
        - Asymmetric
            - public sender – E
            - private – recipient – D
        - Asymmetric and Symmetric
            - Asymmetric share session key
        - S/MIME
            - email apps commonly use, rest and in transit
            - RSA – asymm
            - AES – symm
            - require PKI
        - PGP/GPG
            - both asym and sym
            - RSA
- HTTP Transport Encryption
    - SSL versus TLS
        - TLS replaced SSL
        - both certificate based authentication
        - both asym and sym
    - Encrypting HTTPS Traffic with TLS
        - both sym (session data) and asym (share key for session)
    - Cipher Suites
        - combination algorithms that add security layers to TLS/SSL
            - provide encryption, authentication, and integrity
        - over 200 – ID'd with hex string
            - denote protocol, key exchange method, authentication, encryption, and integrity
    - Implementation Versus Algorithm Selection
        - Crypto Module – hard/soft/firmware that implements crypto functions
        - Crypto Service Provider – software library of cryptographic standards and algorithms
            - used by developers
            - admins implement cyber suites
    - Downgrade Attacks on Weak Implementations
        - forces a system to downgrade its security by configuring server as incompatible with TLS, forcing victim server to use vulnerable SSL
            - allows for POODLE attack
                - prevented by victim server disabling SSL option

- Exploring PKI Components
    - request, create, manage, store, distribute, and revoke digital certificates
        - asymmetric needs Cas

- Certificate Authority (CA)
  - issue, manage, validate, revoke certificates
- Certificate Chaining and Trust Models
  - root certificate – first create by CA and placed in a store
    - if root in store, all subsequent certificates from root can be trusted
  - Trusted Root Certification Authority Store
  - Hierarchical Trust Model
    - CA → Root Cert → Intermediate Certs → Child Certs → Devices/End Users
    - varies on organization size
  - Web of Trust/Decentralized Trust Model
    - PGP/GPG
    - self-signed with third-party voucher
- Registration and CSRs
  - create pub/priv key pair
  - create Certificate Signing Request (CSR) using PKCS #10
  - CA validates and issues cert
    - sometimes request object ID'ers (OIDs) within CSR for certain items
- Revoking Certifications
  - valid to/from dates
  - key pair compromise
  - CA compromise
  - CSR revocation
  - Cert Revocation List (CRLs)
- Certificate Issues
  - expired, not trusted, improper cert/key management
  - online certificate states protocol in real time
- Public Key Pinning
  - prevents attacks from impersonating a website using fraudulent certificates via extra header response
    - contains valid public key hashes and max-age field
- Key Escrow
  - place copy of private key in safe environment
    - recovery – third-party
- Recovery Agent
  - recover private keys recover/restore crypto keys
  - BitLocker
    - recovery agent field
- Comparing Certificate Types
  - machine/computer – ID within domain
  - user, self-signed
  - email
  - code signing
  - wildcard
  - SAN (Subject Alternative Name) – different domains owned by same organization
  - Extended Validation
    - prevent phishing and impersonation attacks
- Certificate Formats
    - X.509v3
    - X.509v2 – revocation
    - CER-binary
    - DER-ASCII

- stored binary or base64 ASCII
- canonical encoding rules (CER) or distinguished encoding rules (DER) → ITU-T X.690 (ASN.1 variant)
    - PEM – privacy enhanced email
    - P7B – PKCSv7 – DER-based ASCII
    - P12 – PKCSv12 – CER-based
    - PFX – P12 precursor used to import/export certs

---

Chapter 11 – Implementing Policies to Mitigate Risks

- Exploring Security Policies
    - form of administrative control
        - ensure security is considered and implemented throughout company system life cycles
    - brief – high-level statements
        - create plans and procedures
        - SOPs
    - Personal Management Policies
        - behavior, expectations, consequences, acceptable use, vacation, separation of duties, job rotation, clean desk policies
    - Acceptable Use Policy
        - as well as use monitoring, expectation of privacy via policy statement
            - read and sign
    - Mandatory Vacations
        - increases likelihood of discovering illegal activities by employees
    - Separation of Duties
        - prevents any single person or entity from being able to complete all of the functions of a critical or sensitive process
        - development vs deployment
        - user rights and permission review
    - Job Rotation
        - helps prevent and/or expose dangerous shortcuts or fraudulent activity
    - Clean Desk Policy
        - ensure protection of sensitive data against theft or exposure
    - Background Checks
        - credit, social media, etc
    - NDA
        - protect proprietary information
    - Exit Interview
        - gain info from employee
        - ensure accounts are disabled
        - collect equipment
    - Onboarding
        - granting access to resources
            - least privilege
        - offboarding
    - Policy Violations and Adverse Actions
        - warning, verbal/written
        - termination
        - avoid overly specific in policy document
    - Other General Security Policies

        - social media and email use
    - Social Media Network and Applications
        - inadvertent information disclosure
            - PII
    - Banner Ads and Malvertisements
        - flash applets with malicious code
        - redirects and drive by downloads
    - Social Networking and P2P
        - consumes bandwidth
        - data leakage and mining
        - inappropriate data hostings
- Agreement Types
    - Interconnection Security Agreement – NIST SP800-47
        - specifies technical and security requirements for planning, establishing, maintaining, disconnecting a secure connection between two entities
    - Service Level Agreement
        - company and vendor
        - performance expectations
    - Memorandum of Understanding/Agreement
        - intention of two or more entities to work toward a common goal
        - less technical/formal than an SLA
    - Business Partners Agreement (BPA)
        - details relationship between partners, obligations
        - ID shares of profits and losses, continuity, etc.

- Protecting Data
    - Information Classification
        - ID, classify, label to understand value
            - public
            - confidential
            - proprietary
            - private
    - Data Sensitivity Labeling and Handling
            - so users know what is being handled and processed
        - Data Destruction and Media Sanitation
            - purging, file shredding, wiping, erasing/overwriting, burning, paper shredding, pulping, degaussing, pulverizing
        - Data Retention Policies
            - how long and where data is stored for
                - beholden by law
        - PII and PHI
            - need two or more pieces for it to be PII
            - minimize use, collection, retention of PII
        - Protecting PII and PHI
            - laws and policies on handling, retaining, redistributing PII with relevant regulation
            - report data losses
            - data classification and labeling, training
        - Legal Compliance Issues
            - HIPAA
            - GLBA

        - SOX
        - GDPR
    - Data Roles and Responsibilities
        - owner – classification, labels, security controls
        - steward/custodian – backups, labels, storage
        - privacy officer – compliance
    - Responding to Incidents
        - adverse events that can negatively affect CIA of data/systems of an organization or has the potential to
        - NIST SP 800-61 rev. 2
- Incident Response Plan
    - define incident types
    - cyber response teams – CIRT
    - roles and responsibilities
    - escalation
    - reporting requirements
    - exercises
- Incident Response Process
    - Incident Response Policy
        - IP Plan
            - Training and Tooling
                - preparation
                - Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned
- Implementing Basic Forensic Procedures
        - collect and analyze evidence
            - prevent modification, control evidence
        - evaluate
            - FTK- by Access Data
    - Order of Volatility
        - order of evidence collection
            - RAM, cache memory, paging file, local disk drives, remote systems, archived media
    - Data Acquisition and Preservation of Evidence
        - capture system image – contents of drive
            - forensics are exact copies without modification
                - Linux “dd” command
            - avoid modifying original evidence
        - Take hashes
            - proof of retained integrity
        - Network traffic and logs
            - matching MACs via NICs
            - protocol analyzers
            - logs
        - Capture Video
            - CCTV
        - Record Time Offset
            - offset between GMT and actual timezone
                - times on a tape recording
                    - timestamps
        - Screenshots

- Witness Interviews
- Chain of Custody
    - collecting and protecting evidence to record possession and change of hands
        - secure storage
- Legal Hold
    - court order to maintain different types of data as evidence
        - preservation
        - data retention policy
- Recovery of Data
    - recovery, unformatting, undeleting
- Active Logging for Intelligence Gathering
    - gather data on attackers
    - vary logging intensity by need/context
- Track Man-Hours and Expense
    - budgeting, quantitative risk assessments, cost evaluations

- Providing Training
    - Role-based Awareness Training
        - data owner – classification/labeling/security controls
        - system admin – overall security
        - system owner – overall responsibility
        - users – understand common threat, training/education
        - privileged user – training on proper handling
        - executive user – risks, overall awareness
        - incident response team – specialized training
    - Direct Senior Management Support
        - Continuing Education
            - regular intervals – stay up to date
        - Training and Compliance Issues
            - best practices
            - standards (PCI DSS)
        - Troubleshooting Personnel Issues
            - insider threat, personal email, policy violations, social engineering, social media
            - data loss prevention techniques, audits, reviews, management response and enforcement
            - education, awareness, training

---

END

---