Security+ Basic Notes -- Not to be used as a primary study source!

Security Basics

Confidentiality (**C**IA)

- Encryption - Turns the message into a code
- Access Controls
    - Identification me
    - Authentication - Password
    - Authorization - Permissions
- **Steganography**
    - Hidden messages in plain site.
    - Hidden text in the file or a photo

Integrity (C**I**A)

- Ensured data is not tampered with
- **Hashing** - Creating a derivative code through an algorithm
    - If data is changed, the future hash will too
- **Digital Signatures, Certificates, and Non-Repudiation**
    - By sending a unique digital signature, you make it clear who sent the message, which allows the receiver to trust it, and the sender to be held accountable.
    - Other forms of Non-Repudiation include tracking, by user account, who did what on a system.
    - **PKI - Public Key Infrastructure**
        - Enables signatures and certificates to function by maintaining encryption keys and certificate management

Availability (CI**A**)

- **Redundancy and fault tolerance** set to ensure that data is retrievable when it's needed
- **SPOF - Single Point of Failure**
    - Any juncture where, if the SPOF fails, the whole system ceases to function
- **Disk Redundancy**
    - Raid 1, 5, 6, 01, 10
- **Server Redundancy**
    - Extra clusters! If one server fails, it fails over to the redundant server
    - Virtualization can help

- **Load Balancing**
    - Multiple servers supporting a service so one doesn't get overloaded
- **Site Redundancies**
    - If a fire or flood takes out one location, another backs it up
        - **Hot Site -** Ready and available 24/7
        - **Cold Site -** Location where equipment, data, and personnel can be moved to when needed
        - **Warm Site -** Mix between hot and cold site
- **Backups**
    - Data stored in multiple places
- **Alternate Power**
    - UPS and generators
- **Cooling Systems**
    - HVAC
- **Patching**
    - Keep systems bug free and clear of security issues

Safety

- **Safety of People -** Emergency escape plans, drills, and training
    - Often, secure facilities will unsecure in case of emergency to ensure human safety
- **Safety of Assets -** Physical security measures like locks, lighting, fencing, CCTV, and more

Layered Security/Defense

- No single approach is enough- mix and match!
- Every step, layer, and phase needs its own security protocols
- **CAC - Common Access Card**
    - Smart card including readable ID info for secure environments
- **PIV - Personal Identity Verification**
    - Smart card including readable ID info for secure environments
- **HOTP- HMAC-based One-Time Password**
    - An example of a rolling key-based password like the ones used in tokens.
    - HOTP passwords are usable once only, but theoretically forever until used
    - Open-source and affordable systems
    - **TOTP - Time-Based HOTP**
        - Duh

Authentication Services

- **Kerberos**
    - Functions on Unix and Windows Active Directory Domains
    - Prevents MitM attacks through use of mutual authentication
    - Uses tickets to prevent repeat incidents
    - **Requirements**
        - **KDC- Key Distribution Center**
        - **TGT- Ticket Granting Tickets**
            - Certificates are packaged within digital authentication “tickets” or tokens
        - **Time-Stamping and Synchronization**
            - Tickets are only valid for a certain amount of time, so systems must be within 5 minutes of each other.
            - Time-outs prevent replay attacks
            - **Replay Attacks**
                - Intercepted authentication data so third party can connect
    - **Uses Symmetric Key Cryptography**
        - One key encrypts and decrypts
- **Asymmetric Encryption Key**
    - Utilizes two keys- a public encryption key (hosted by PKI) and a private decryption key.
- **LDAP and Secure LDAP - Lightweight Directory Access Protocol**
    - X.500 based that (when secure) can use TLS
    - Specifies formats and methods to query a directory of objects (users, computers, and directory objects)
    - **Microsoft Active Directory** is based off LDAP
    - Enables a single location to interact with all resources on a directory
    - **Secure LDAP**
        - Utilizes **TLS - Transport Layer Security *Session*** to encrypt data
        - Secure LDAP v2 used SSL encryption, but v3 uses TLS
- **SSO - Single Sign On**
    - Feature enabled in both Kerberos and LDAP, wherein a user signs into the network once and receives a token which can sign them into all necessary systems
    - **Federations**
        - Enables two non-homogenous networks to coordinate permissions for users
        - User holds credentials on both networks, but signs into the federation which treats them as a single account

    - **SAML - Security Assertion Markup Language**
        - **XML based**
        - Allows websites to enable federation like trust privileges so that users can access resources on both
        - **Principal -** User
        - **Identity Provider -** Identity management utility - contains IDs and passwords
        - **Service Provider -** Serves principles - redirecting to different hosts or domains
- **RAS - Remote Access Service Authentication**
    - Accessed via dial-up or VPN
    - **PAP - Password Authentication Protocol**
        - Cleartext, insecure, single authentication
        - Utilizes **PPP - Point-to-Point Protocol**
            - Used clear-text because over dial-up, nobody thought wiretaps a legitimate risk
    - **CHAP - Challenge Handshake AP**
        - Server challenges client, can happen multiple times a session
        - More difficult to crack because of a hashed code at the start of session
    - **MS- CHAP**
        - Microsoft's CHAP
    - **MS-CHAP v2**
        - CHAP + Mutual authentication
    - **RADIUS - Remote Authentication Dial-in User Service -**
        - *Centralized* method of authentication for multiple remote servers
        - Encrypts password, but not the whole authentication process
        - Utilizes UDP for best effort connection
    - **Diameter**
        - A fucking pun
        - RADIUS but utilizes EAP for better encryption
        - Utilizes TCP for guaranteed connections
    - **XTACACS - Extended Terminal Access Controller Access-Control System**
        - Cisco proprietary TACACS improvement
        - Outdated
    - **TACACS+**
        - Cisco proprietary alternative to RADIUS.
        - Interoperable with Kerberos.
        - Works on a wide host of environments
        - Encrypts full authentication
        - Uses TCP for guaranteed connections
        - Also used to secure network devices like routers by corporations
    - **AAA Protocols**
        - **Authentication**

        - Proves your identity
    - **Authorization**
        - Determines what you should be able to access
    - **Accounting**
        - Tracks what you do
    - Radius and TACACS+ are AAA protocols, and Kerberos is considered one, though it does not have accounting.

Control Implementation Methods

- Technical Controls: Utilizes Technology
- Management Controls: Use administrative or management methods
- Operational Controls: Implemented by people in day-to-day operations

Technical Controls

Technology installed by an administrator that automatically provides protection and reduces vulnerabilities.

- **Encryption**
- **Antivirus Software**
- **IDSs- Intrusion Detection Software**
    - Monitors a host and reports on intrusions
- **Firewalls**
    - Restrict I/O traffic to a server or host
- **Least Privilege**
    - Only allowing each user the minimum privileges they need to limit risk if something goes wrong
- Motion detectors, fire suppression systems, and other such devices are also technical controls which help provide additional physical protection and safety

Management Controls

Also known as administrative controls, these use planning and assessment to reduce risk.

- **Risk Assessment**
    - **Quantitative Assessment**
        - Uses cost and asset values to determine how much it'll cost to protect x-value of assets
    - **Qualitative Assessment**
        - Categorizes risks based on probability and impact
- **Vulnerability Assessment**

    - Used to discover current vulnerabilities and weaknesses to help prioritize the implementation of additional controls
- **Penetration Tests**
    - Actual attempts to exploit vulnerabilities to determine how easy it is to do, and what the actual effects are

Operational Controls

People-implemented practices in compliance with an overall security plan.

- **Awareness and Training**
    - Prevents social engineering, people writing down passwords, etc.
- **Configuration and Change Management**
    - Ensures that each system starts in a baseline of security and that changes do not invalidate security features
- **Contingency Planning**
    - Reduces overall impact if something goes wrong by having prepared responses
- **Media Protection**
    - Don't lose flash drives with valuable shit
- **Physical and Environmental Protection**
    - Cameras, door locks, HVAC systems

NIST - National Institute of Standards and Technology

- Hosts the **ITL - Information Technology Lab**
- Publish **SP 800 - Special Publication 800** which are security standard documents that many IT professionals, and certifications, reference directly
- These are invaluable security standards

Control Goals

- **Preventative** controls
    - **Hardening**
        - Making a system more secure than default by deactivating unnecessary features, creating restrictions, disabling accounts
    - **Security Awareness and Training**
        - Ensuring users are aware of vulnerabilities and social engineering attempts
    - **Security guards**
        - Often will deter potential attackers, can verify identities of people
    - **Change Management**
        - Changes aren't made on the fly, they're studied first
    - **Account disablement policy**

        - If it ain't necessary, nix it
- **Detective** controls
    - **Log Monitoring**
        - For example, firewall logs track everything blocked to help reveal incidents
    - **Trend Analysis**
        - Taking note of an increase of firewall denials, etc
    - **Security Audit**
        - Can detect if users are using good passwords or if users have more rights than they need
    - **Video Surveillance**
        - CCTV yo
    - **Motion Detector**
        - See above?
- **Corrective** controls
    - **Active IDS**
        - Detect attacks and modify environment to stop them
    - **Backups and System Recovery**
        - Fix shit when it breaks
- **Deterrent** controls
    - **Cable Locks**
        - If its hard to take, its less likely to be taken
    - **Hardware Locks**
        - … ITS A LOCK
- **Compensating** controls
    - Temporary controls while implementing other things, or when other things go bad

Physical Security Controls

- **Perimeter**
    - Get a big ‘ol fence like the military
- **Building**
    - Four walls and a big ‘ol locked door
    - Some of these even have LIGHTS holy crap wow such security
- **Secure Work Areas**
    - Don’t let people in that aren’t supposed to be there
- **Server and Network Rooms**
    - Only let the IT nerds in, use bigger locks
- **Hardware**
    - MORE LOCKS

Doors

- In general have less points of entry with more locks, security guards, cameras, biometrics, and laser beams. But like, be careful of trapping your employees in there when the place sets on fire.
- **Cipher Locks**
    - Press buttons in the right order and the door opens
    - These aren't really all that secure, but you can make them harder to crack
- **Proximity Cards**
    - Door shoots the card with lightning and if the card goes, "YEAH!" the door opens
    - You can identify people with special cards
    - Prox cards are pretty easy to steal info from, but a few pieces of aluminum in your wallet can fuck that up
- **Biometrics**
    - USE YOUR FUCKING EYEBALL AS A KEY
    - This allows identification
- **ID Badges**
    - Do you look like your picture or nah
- **Tailgating**
    - Stop holding doors open for other people chivalry is dead let them use their own security credentials you white-knight piece of crap
    - **Man traps** are cool
- **Access Lists and Logs**
    - Track who goes in, and have guards only let certain people in
    - If someone exits a building, but was never logged into the building, they probably tailgated so fire them
    - Video surveillance is a good partner
        - It's best for proof. It's hard to deny footage, but people can tailgate or use each others credentials
- Motion Detectors + Fences mean you know when someone climbs it
- Motion detectors can also modify lighting so you can save money but still be secure
- Alarms are annoying but secure
- **Barricades** can make vehicles and people zigzag in, giving more time to prevent or identify them
    - **Bollards**, or short vertical polls, look better than heavy barricades but still prevent people from driving through your walls
- **No Trespassing** signs supposedly work
- **Locks, laptop locks, locking cabinets, and safes.**

Logical Access Controls

- **Least Privilege** - Only give users access to what's essential

- **Group Policy** - Allows you to change a setting once and have it affect whole groups
- Most notes weren't taken because info is fairly obvious

Access Control Models

- **Subjects**
  - Users or groups
- **Objects**
  - Files, folders, shares, or printers
- **Role-Based Access Control (RBAC)**
  - Instead of assigning permissions to users, assign permissions to specific roles, and assign roles to specific users.
  - The *Microsoft Project Server* operates like this with four chief roles
    - *Administrators* - Can access anything and adjust settings
    - *Executives* - Can access anything but have no control over settings
    - *Project Managers* - Full control over data and settings within their project
    - *Team Members* - Can only report on work that was specifically assigned to them by project managers
  - These systems can often be seen as hierarchical, as higher-level accounts have more access
  - Matrix planning documents set up tables explaining the permissions before the roles have been created to make sure they make sense and cover all possibilities
- **Rule-Based Access Control (RBAC)**
  - Such as when firewalls and routers use **Access Control Lists (ACL).**
  - Static Rules such as allow or disallow traffic on a specific port
  - Dynamic Rules
    - When in IDS adjusts rules to block specific traffic
    - When Marge has more permissions when Homer is absent
- **Discretionary Access Control (DAC)**
  - Every file/folder has an owner who sets who can and can't access/modify/view
  - NTFS is known for this
    - Every NTFS object has a **DACL** (Discretionary ACL) which notes the SID (Security ID) of users
    - DACL is filled with Access Control Entries (ACE) which contain an SID and associated permissions
  - *Trojan Risk* if you install malware with Admin priveleges, that malware can continue to operate with those same priveleges
- **Mandatory Access Control (MAC)**
  - Operates under the principle of least privilege
  - Both users and objects have sensitivity labels, and only if the user has equal or greater label, AND need to know, can they access the file

    - In high security situations, multiple levels of checks are enabled before deciding a user is need to know in any given matter
    - This system is slow and inflexible, but very secure

Network Security

Protocols

Basic Connectivity Protocols

- TCP - Handshaked session-oriented communication
- UDP - Best effort communication
- IP - Host identification
- ICMP - Basic connectivity, traceroute, ping
    - Can cause DoS vulnerabilities
- ARP - IPv4 to MAC address
    - ARP poisoning gives false updates to redirect or interrupt traffic
- **NDP - Neighbor Discovery Protocol**
    - IPv6 protocol similar to ARP, also identifies default gateway and performs other autoconfiguration efforts

Encryption Protocols

- SSH - Encrypts **SCP - Secure Copy** and **SFTP - Secure File Transfer Protocol** among a wide variety of others.
    - SSH can also encrypt TCP Wrappers, a type of access control list on Unix systems
    - Uses port 22
- SCP - Based on SSH and copies encrypted files over a network
- SSL - Secure Socket Layer
    - Secures HTTP into HTTPS with the use of certificates
    - Can also secure SMTP and LDAP
    - ***TCP 443 for HTTPS***
    - ***TCP 465 for SMTPS***
    - ***TCP 636 for LDAP with SSL***
- TLS - Transport Layer Security
    - Designated replacement for SSL
    - Same ports as SSL
- IPsec
    - Encrypt IP traffic
    - Native to IPv6 but works on IPv4
    - Encapsulates and encrypts packets and then uses tunnels to protect VPN traffic

    - **Authentication Header - AH -** Protocol ID number 51
    - **Encapsulating Security Payload (ESP) -** Protocol ID number 50
    - Uses **Internet Key Exchange (IKE)** over UDP 500 for VPN security

Application Protocols

- HTTP
    - Port 80
- HTTPS
    - Port 443
- FTP
    - 21 for connection
    - 20 for data
- SFTP - Secure File Transfer
    - 22 for data because it uses SSH
- FTPS - File Transfer Protocol Secure
    - Like SFTP but uses SSL or TLS
    - ***Ports 989 or 990***
- TFTP - Trivial File Transfer
    - UDP port 69
- Telnet - Outdated CLI based remote connection protocol
    - Sometimes still used to connect to routers
    - Cleartext, insecure
    - Port 23
    - **PuTTY** operates similarly to telnet but includes SSH
- SNMP - Simple Network Management Protocol
    - Monitors and manages network devices like routers and switches
    - Sends requests to SNMP agents on devices on UDP 161
    - Receives info back from agents on UDP 162
- NetBIOS
    - Allows for basic LAN identification and sessions
    - UDP Ports 137 and 138
    - TCP Port 139, and rarely 137
- LDAP
    - Communicates with directories like Microsoft Active Directory and Novell Network Directors Services (NDS)
    - Provides a single location for object management
    - ***TCP 389***
    - When encrypted with ***TLS or SSL, Port 636***
- Kerberos - Authenticates in Windows domains and some Unix environments
    - Uses KDC - Key Distribution Center to issue timestamped tickets
    - UDP Port 88
- Microsoft SQL Server

    - SQL server hosts databases that web servers and applications use
    - ***Port 1433***
- RDP - Remote Desktop Protocol
    - Connect to systems from remote locations
    - Used in Remote Desktop Services and Remote Assistance
    - ***TCP or UDP 3389***

E-mail Protocols

- SMTP
    - Transfers email between client and SMTP server
    - TCP port 25
    - Secure SMTP with SSL or TLS uses ***Port 465***
- POP3
    - Transfers emails from servers to clients
    - TCP 110
    - Secure POP3 with SSL or TLS uses ***TCP 995***
- IMAP4
    - Stores email on a server
    - Allows user to organize and manage email in folders on server
    - TCP 143
    - Secure IMAP4 with SSL or TLS uses ***TCP 993***

Assorted DNS

- DNS uses UDP 53 for URL queries
- DNS uses TCP 53 for zone transfers- when name servers exchange updated records
- DNS uses **BIND - Berkley Internet Name Domain** software on Unix/Linux servers

Ports

- **IANA - Internet Assigned Numbers Authority** maintains a list of official port assignments
- Ports are default routes that different protocols use for data- this allows administrators to block certain protocol interactions just by closing or opening ports
- 65,535 UDP and TCP ports
- **Well-Known Ports 0-1023**
- **Registered Ports 1024-49151**
  These can be registered by single companies for proprietary use, or by multiple companies to establish a standard.
- **Dynamic and Private Ports: 49,151-65,535**
  Any application can use these and they can be temporarily mapped

- Most attacks are on well-known ports
- Port scanners check what ports are open and then know which data can be tampered with
- **Protocol IDs are not to be confused with ports**.
  You can allow or block traffic by the protocol ID, but the ID does not match up with ports.

Protocol	Port	Protocol	Port
FTP data port (active mode)	TCP 20	NetBIOS (TCP rarely used)	TCP/UDP 137
FTP control port	TCP 21	NetBIOS	UDP 138
SSH	TCP 22	NetBIOS	TCP 139
SCP (uses SSH)	TCP 22	IMAP4	TCP 143
SFTP (uses SSH)	TCP 22	LDAP	TCP 389
Telnet	TCP 23	HTTPS	TCP 443
SMTP	TCP 25	SMTP SSL/TLS	TCP 465
TACACS+	TCP 49	IPsec (for VPN with IKE)	UDP 500
DNS name queries	UDP 53	LDAP/SSL	TCP 636
DNS zone transfers	TCP 53	LDAP/TLS	TCP 636
TFTP	UDP 69	IMAP SSL/TLS	TCP 993
HTTP	TCP 80	POP SSL/TLS	TCP 995
Kerberos	UDP 88	L2TP	UDP 1701
POP3	TCP 110	PPTP	TCP 1723
SNMP	UDP 161	Remote Desktop Protocol (RDP)	TCP/UDP 3389
SNMP trap	UDP 162	Microsoft SQL Server	TCP 1433

Basic Assorted Network Security

- Switches are more secure than hubs because they limit where traffic is sent and received, thus disabling sniffers
- Switches can be affected by loops- when a cable is connected needlessly between two ports, and data is unicast looped through the connection
  - STP (Spanning Tree Protocol) and RSTP trivialize this risk by not letting routing suck that bad
  - STP also protects against attacks because a jerk could always just mess with two rj45 jacks and slow down the whole network
- Switches can also group several computers into a VLAN, isolating network traffic
  - This allows people who are not in the same physical proximity to work together securely
- Physical ports that are not being used can also be disabled on the switch to prevent people from connecting to the network
- Mac address filtering can also accomplish this, where a port only accepts specifically named mac addresses for connections
- **802.1x** is much better security than mac address filtering or physical port disabling.
  - Works as RADIUS or Diameter user
  - Requires authentication to connect

    - Can customize features, such as allowing non-authenticated users internet access, but no local data

Routers

- Routers don't pass broadcasts, so segments separated by routers are broadcast domains
- Routers allow the use of ACLs (just like firewalls) to identify allowed traffic
    - This filtering can be for IP addresses, ports, protocols
    - This means you can block traffic from specific computers or network segments
    - Implicit Deny is pretty important for security, and insists that anything not specifically allowed is denied

Firewalls

- Offer similar ACL based security features as routers
- A brick wall between inside and out that prevents certain kinds of traffic.
- Advanced firewalls that fall under "Unified Threat Management" can do much more than simple packet filtering
- **Host Based Firewalls** operate for a single host and can prevent invasions and exploitation through an NIC
    - These are essential when using public wifi
- **Network Based Firewalls**
    - Controls traffic going in and out of larger network segments
    - Best between internal network and internet
    - Usually a dedicated system with monitoring, filtering, and logging
    - *Sidewinder* is a dedicated server with proprietary firewall software
- **Rules**
    - Similar to routers ACL
    - Permit/Allow or Deny
        - Protocol ID/Port
        - Source
        - Destination
    - When configuring, start with implicit deny, and allow all traffic that you know you want
- **Web Application Firewall (WAF)**
    - Specifically protects web apps hosted on a server
    - Blocks traffic such an NOOP sleds and NOOP ramps
    - Detects malicious code sent to web server
- **Advanced Firewalls**
    - **First Gen -** Packet filtering rules, stateless- works only according to ACL
    - **Second Gen -** Stateful inspection- tracks sessions and inspects traffic based on session status

    - **Third Gen** - Application Level firewalls. Aware of specific commands used in apps or protocols. WAF are third gen that inspect HTTP.
    - **Next Gen** - Closer to UTM and frequently adding new features
- **Firewall Logs and Analysis**
    - Log all allowed traffic, all blocked traffic, or both
    - Scripts and apps make it easier to review logs
    - IDS use firewall logs to identify intrusions
        - For example, a port scan attack will query lots of well known logical ports. If logs are enabled, this is visible and can be used to prevent further attacks

Protecting the Network Perimeter

- **DMZ**
    - A section of the network available to external hosts, but segmented and secured so that it does not allow access to secure local data
    - Mail servers are often in the DMZ but surrounded by firewalls on both sides
    - Often servers within the DMZ can communicate with internal hosts/servers in order to relay info while remaining secure, because this requires special permissions with the second firewall
- **NAT and PAT**
- **Proxies**
    - Can cache content for easier access, or restrict content with advanced filtering
    - Exists on the far edge of the intranet, but typically only filters HTTP and HTTPS, though its capable of also filtering protocols like FTP
    - Filtering is typically through URL filtering, which blocks specific websites.
        - Many services sell lists of URLs that fit under certain categories a company may want to block
    - Proxie servers also watch and log everything, so be careful dummy
- **Unified Threat Management**
    - All-in-one tools with antivirus, url filtering, etc
    - **Web Security Gateway**
        - Blocks malware in email or webpages and spam
        - Often include firewall capabilities
        - Their golden tool is content filtering, where they analyze all packets for malicious code
        - Cisco sells **WSA - Web Security Appliance** which even includes Data Loss Prevention which means it scans outgoing data for confidential info as well
    - **UTM Security Appliance**
        - “Just works” all-in-one UTM
        - **URL Filtering**
        - **Malware Inspection**

        - **Content Inspection**
    - Very little difference between the two, and most are just referred to as UTM

Advanced Network Security

- **IDS - Intrusion Detection Systems & IPS**
    - Typically only detect and notify, though some active IDS can take steps to block attacks
    - Either detect predefined attack signatures or note anomalous behavior
        - Anomaly-based first establishes a baseline of normal operation, and notes when it changes
        - Anomaly-based is good at detecting zero-day issues that haven't been identified yet
        - Anomaly-based requires regular updating of baseline after system or network changes in order to remain accurate
    - **HIDS - Host Based**
        - Installed on individual servers or workstations
        - Primarily monitors traffic through NIC
        - Many now also monitor application activity on a system
        - HIDS can identify malware that some antivirus would miss
            - Many organizations install a HIDS and antivirus on every workstation
    - **NIDS - Network Based**
        - Installed on network devices like routers or firewalls
        - Installed on network devices but report to central monitoring server with a NIDS consol
        - NIDS don't detect anomalies on individual hosts unless they're dire, and cannot decrypt data
        - Mostly analyze larger network trends and plaintext transmissions
        - You can place NIDS sensors at different points in a network configuration to detect different kinds of issues, such as what attempts are made vs. what attempts get through the firewall
        -
    - Passive IDS logs an alert and may notify personnel
    - Active IDS logs and notifies personnel, but also changes the rules of the environment accordingly
    - An IPS is always placed in-line with traffic so it can prevent the success of an attack
    - IDS and IPS utilize packet sniffing for info gathering
        - Physical sniffing requires being plugged in
        - Wireless sniffing can intercept over the air

    - **SYN Flood Attack**
        - Example of DoS
        - Repeatedly sends the initial Syn packet in a handshake, but never sends the final ack
        - All of these incomplete sessions drain resources until the server crashes, or the server begins denying legitimate connections
        - IDS and IPS can detect these attacks, and many firewalls include a flood guard that will detect the attacks and close the open sessions
- **Honeypots**
    - Utilize basic security to offer a tantalizing vulnerability
    - Typically filled with bogus data and fake transactions
    - Good way to gather info on an attacker
    - Two Goals: Distract, and Analyze
    - **Honeynet**
        - Virtualized servers that work like a live network
        - Even more tantalizing and distracting
        - Provides more time to assess the attacker
- **Don't Counterattack**
    - Attackers have more time than you, and possibly more skill than you. Don't piss them off
    - You also run the risk of attacking a fellow victim, rather than the attacker himself
- **Using Multiples NIPS**
    - You can put NIPS 1 between the internet and the local web/mail servers
    - NIPS 2 goes between those servers and another batch of internal private network.
    - This means that if malware sneaks past the first wall, it can't launch attacks directly at everything- it's cordoned off.
    - **Advance Persistent Threats (APTS)**
    - **RATs (Remote Access Tools)**

Securing WLAN

Misc Wireless Principles

- Antennas
    - **Isotropic**
        - Theoretical perfect 360 horizontal/vertical spread
        - Most omnidirectional antennas try to emulate this
    - **Dipole**
        - Most common, 360 horizon, 75 vertically
        - Looks like a normal pencil antenna
    - **Yagi**

        - Dipole antenna with additional director element
    - dBi/dBd indicate the gain of the antenna based on its physical characteristics
    - dBm indicates the power level of the WAP and can be adjusted
    - Not all WAPS are routers, some just allow access to the network
    - Users want good coverage, administrators want low coverage for security
    - Lol most of this can be thwarted by throwing a can around an antenna to make a long range antenna
- **Security Protocols**
    - WEP
    - WPA
    - WPA2 - IEEE 802.11i
        - Wi-fi Alliance requires all Wi-Fi Certified devices to meet WPA2 standards
        - This includes Counter Mode with **Cipher Block Chaining Message Authentication Code Procotol (CCMP)**
        - WPA2 has theoretically been cracked, but a 20 character complex key should work.
    - Authentication with Enterprise Mode
    - **TKIP v CCMP**
        - **Temporal Key Integrity Protocol TKIP** was used with WPA before CCMP
        - Each packet in TKIP gets a new key, making it more secure than WEP
        - Some WPA security uses AES instead of TKIP, which is pretty secure, so on hardware that only supports WPA it can be a solution
    - 802.11x in implemented as a RADIUS or Diameter server, and can be used with WPA or WPA2 using enterprise mode
        - WPA/WPA2 in personal mode just use a pre-shared key, which doesn't authenticate.
        - Enterprise mode authenticates users, who have individual sign-ons and passkeys
        - **RADIUS uses port 1812, but occasionally 1645**
    - **EAP -** A system to create a secure encryption key, known as **PMK - Pairwise Master Key**.
        - Used by both TKIP and AES-based CCMP
    - **PEAP -** Encapsulates and encrypts the EAP conversation in a TLS tunnel
        - MSCHAPv2 uses this
        - Requires certificate on server, but not on clients
    - **EAP-TTLS** - Allows older authentication methods such as PAP within a TLS tunnel
    - **EAP-TLS -** Most secure EAP standards and widely used. Requires certificates on the 802.1x server and each client.
    - **Lightweight EAP (LEAP) -** Modified version of CHAP. Doesn't require digital certificate, and less secure.
    - Small device security

        - **WTLS - Wireless Transport Layer Security**
        - **ECC - Elliptic Curve Cryptography**
    - **Captive Portals**
        - Those annoying websites that make you sign into the network.
    - **Hotspots with Isolation Mode**
        - Isolation mode prevents people from accessing or sharing data across a network. This is good to provide users with internet access in an unsecured fashion
    - **Mac Filtering**
        - Limit wireless access to specific Mac addresses
        - This isn't that useful, as sniffers can spoof their mac address to an allowed one
- **Wireless Attacks**
    - War driving
    - **War Biking**
        - Security guy went around with an unsecured hotspot to collect user data. In two days, 2900 people logged into it.
        - He found most used unsecured wireless that he could easily impersonate
    - There's no reason to disable SSID as anyone who cares can figure it out easily
        - You can at least hide it from casuals
    - **WEP/WPA attacks**
        - WEP uses the RC4 stream cipher and reuses encryption keys, so its easy to find that key and gain full access
        - **IV attacks**
            - The encryption key is created by combining the WEP with an IV -initialization vector. But this IV is sent to the client in plaintext
            - This IV range is limited, and easily cracked
            - Packet injection (making it send more response packets) can make cracking take less than a minute
        - **WPA Cracking**
            - 1, Use a wireless sniffer to capture wireless packets
            - 2, Wait for client to authenticate, and steal the encrypted passphrase
            - 3, Use a brute force attack, offline the user can break the encryption on that passphrase and then go back online once they have that passphrase
            - If nobody is active on a wireless, it can't be cracked. But if someone is active, the attacker can disconnect someone and steal the encrypted passkey when they try to reconnect.
        - **WPS cracking**
            - Super easy. The pin can be guessed in ten hours
    - **Rogue Access Points**
        - A WAP placed by an attacker meant to look friendly

    - **Evil Twin**
        - A WAP meant to impersonate a friendly WAP
    - **Near-Field Communication**
    - **Bluetooth Jacking**
        - Don't let someone connect to you while in discovery mode
        - **Bluejacking -** Sending unsolicited messages to a device over bluetooth
        - **Bluesnarfing -** Data theft over bluetooth
        - **Bluebugging -** Taking over a device through bluetooth to log phone conversations, forward calls, send messages, etc

Remote Access

- Dial-up RAS
    - Uses POTS and modems and PPP
    - Not secure if lines are tapped
- **VPN and VPN Concentrators**
    - VPN Concentrators, often housed on VPN servers, provide all the tools required to run the VPN, including encryption and authentication.
    - VPNs allow you to run tunnels through public spheres to logically separate and secure traffic.
    - **IPsec and VPN**
        - IPsec offers both Tunnel Mode and Transport Mode
        - **Tunnel Mode** is used with VPN, and encapsulates the entire IP packet
        - **Transport Mode** only encrypts the payload and is more efficient in private networks
        - IPsec also uses **ESP (Encapsulating Security Payload)** to encrypt data and provide confidentiality. ESP uses protocol ID 50
        - IPsec uses the **IKE (Internet Key Exchange) Protocol** over ***port 500***.
            - Between the PID and that port, there are lots of ways to customize ACL rules regarding IPsec
    - **L2TP** is a good tunneling protocol, but does not encrypt data. IPsec can work in conjunction with L2TP for a very good tunnel
    - **IPsec and NAT issues**
        - NAT and IPsec are incompatible
        - Instead of IPsec, you can use tunneling protocols that rely on SSL or TLS
        - **SSTP - Secure Socket Tunneling Protocol** encrypts VPN traffic over SSL using port 443
            - OpenVPN and OpenConnect are similar programs that use TLS
    - **PPTP - Point To Point Tunnelling Protocol**
        - Uses Microsoft's encryption
        - Unused today because of known vulnerabilities
        - Uses **TCP Port 1723**
    - **Site-to-Site VPN**

        - Uses two VPN servers in different locations to form gateways
        - From user end, its as if there's a single network
        - Can be slow
    - **VPN over Open Wireless**
        - Two easy methods to secure yourself over open wireless
        - HTTPS connections only
        - Apps like Private Internet Access or TunnelBear that provide VPN services over open wifi
    - **NAC - Network Access Control** is essential on VPNs, because Admins lack complete control over home user computers, so they need to be able to restrict data and traffic somehow
        - **Health and Control**
            - Systems can be assigned health status based on how updated their antivirus definitions are, how updated their OS is, and the status of their personal firewall
            - When a client accesses a VPN, an authentication or health agent queries the status of that client
            - If the client doesn't meet health standards, they can be put on a quarantine network including resources to upgrade the health of that client
            - For local clients, this may mean they have internet access, but cannot communicate with other devices on the network

Securing Hosts and Data

- OS and Application Hardening
    - Disabling Unnecessary Services
        - If you don't use FTP or RDP, kick them to the curb
        - This Improves Overall Security
        - Reduces Open Port Risks
        - Reduces Attack Surface
    - Eliminate Unneeded Applications
        - Base OS installations have a lot of apps that may be unnecessary or unused in your company. If a major vulnerability goes around for those apps, and your security definitions aren't up, you fucked.
    - Disable default and unused accounts
        - Pay special attention to backdoor accounts that bypass security
    - Protect Management Interfaces
- **Establish Baselines**
    - Set up standards for all computers so that its easier to prepare them for use
    - Set up monitors that check against the baseline to ensure computers remain secure

- Set up NAC and a quarantine server for when things go wrong
- **Security Baselines**
  - Might have requirements like FTP disables, all antivirus up to date, and host-based firewall installed
  - Most organizations will have different baselines for different hosts
  - **Imaging** is cool, cause you configure one computer, and take a "snapshot" of its settings that spread to other computers
    - Symantec Ghost and Windows Server 2012 offer this feature
    - Could be worth taking weeks or months to develop and test the source image
    - This greatly reduces cost and time of deploying new systems, and allows administrators to focus their efforts
    - You can check actual settings on live computers against the image for easy remediation
  - **Group Policy**
    - Forces certain configuration on all devices in a group
    - **Account Settings**
    - **Password and Lockout Settings**
    - **Audit Policies** - logs certain events such as log on/off or file access
    - **User Rights** - such as remote desktop usage or power off privileges
    - **System Services** - disable services like FTP
    - **Software Restrictions** - what software can be installed and/or run
- **Configuration Baselines**
  - Printer config, app settings, TCP/IP settings, etc
  - If something stops working, you can check against baseline to identify the issue
  - Configuration baselines must be kept up to date with new changes in policy
  - **USGCB - US Gov Configuration Baseline**
    - Covers most common security issues and are easy to deploy
    - Good for agencies with limited resources
    - These images are compatible with **SCAP - Security Content Automation Protocol** which verifies security settings are preventing known vulnerabilities
- **Host Software Baselines**
  - What software is on and allowed. Includes ability to scan systems
- **Application Configuration**
  - Settings within an application
- **Performance Baseline**
  - Identifies resource utilization and overall performance to check against future status

    - **Trusted OS**
        - Meets security guidelines, doesn't allow things to run which shouldn't

Virtualization

- Virtual Machines or Networks running on a single physical platform
- **Hypervisor**
    - Software that creates and runs the virtual machine
    - VM-Ware, Microsoft Hyper-V, Windows Virtual PC, Oracle VM Virtual Box
- **Host**
    - Physical server
    - Lots of processors, tons of memory, shit ton of everything
    - Smaller and cheaper than multiple physical machines
- **Guests**
    - Operating Systems running on the host
- **Patch Compatibility**
    - VMs need patched
    - If it works on a physical machine, it'll work on the virtual one
- **Host Availability/Elasticity**
    - The ability to redirect resources to the VM guest that needs it
- **Sandboxing**
    - Creating an isolated testing area that does not affect the physical machine or other VM machines
    - You can test virus, antivirus, patches, software, etc
- **VM Files**
    - **VHD Files**
        - Contains the content of **Virtual Hard Disk (VHD)**
    - **XML Files**
        - Contain configuration of VM as well as snapshots
    - **AVHD Files**
        - Differencing disks- contain the differences between current VHD and snapshots
    - **VSV Files**
        - Similar to hibernate for VM
    - **BIN Files**
        - Memory for systems in a save state
    - Because of VM files, it's easy to move VM from one server to the next, or to backup whole servers
- **Virtual Network Connectivity**
    - Virtual NICs, Virtual switches, and virtual networks
    - You can configure full VLANs on VM servers to segment traffic

    - This also helps testing malware because you can see how it will operate across a network, though some Malware can detect when its in a virtual environment and change its behavior
- **VM Risks**
    - **VM Escape**
        - A very serious threat where a malware program tries to get access to the hypervisor from within the virtual machine.
        - Hypervisor runs with elevated admin privileges, so gaining access to hypervisor allows it to take control of the physical system and all the virtual hosts
    - **Loss of Confidentiality**
        - Because all VM is just files, whole systems can be fairly easy to steal
        - Encrypt every'tang

Patches

- Patches keep software secure, kinda
- Auto-deployment of patches works sometimes, but if a conflict occurs, it can be a serious issue
- Patch tuesday is a big day when microsoft releases patches, so wednesdays are dangerous
- Also if a patch crashes a system, it can crash a thousand. Test out patches on systems very like the deployed systems

Security in Static Environments

- **System Examples**
    - **Supervisory Control and Data Acquisition Systems (SCADA) -** Industrial control systems within power plants and water treatment facility. These are typically disconnected from the internet
    - **Embedded Systems -** Computing components in printers, HVAC, etc. Not usually connected to the internet so unlikely attack vectors, but dangerous if someone figures out how to control them. (Haywire HVAC is lethal)
    - **Mobile Systems -** Smart Phones and such, but becoming much less static.
    - **Mainframes -** High powered systems specific to an organization. Might be contained on isolated networks, but often connected to the primary network so personnel can access it.
    - **Game Consoles**
    - **In-Vehicle computing systems -** Cars can be hacked now cool
- **Stuxnet**
    - Stuxnet was a worm designed to attack a specific embedded system in an Iranian Nuclear Facility
    - It made all the centrifuges spin fast enough to tear themselves apart

    - Methodology:
        - **Infection -** Hidden on a flashdrive
        - **Search** - Worm located the target systems
        - **Update -** Downloaded updated version of the worm
        - **Compromise** - Takes advantage of zero-day vulnerabilities
        - **Control** - Makes the system go nuts
        - **Deceive and Destroy** - send false data to engineers
- **Protecting Static Systems**
    - **Redundancy** - Like RAID, make sure there are backups for failure. This means firewalls from different vendors, SCADA backup controls, etc.
    - **Network Segmentation -** An extreme form keeps all systems off primary network, like SCADA talking to each other, but only that.
    - **Security Layers** - Firewall, NIPS, etc
    - **Application Firewalls -** Can identify specific commands in a protocol, good for services that don't use many protocols
    - **Manual Updates -** Only install verified updates
    - **Firmware Version Control -** keep firmware up to date
    - **Wrappers** - Like TCP wrappers, use these to filter traffic
- **Securing Mobile Devices**
    - **Encryption**
    - **Authentication and Device Access Control -** Username/Password
    - **Locator Services - Lost Mode**
    - **GPS can be used to track you**
    - **Removable Storage Risks -** If you don't encrypt your data, removable storage is easily lost or easily taken
    - **Storage Segmentation -** Keep low-security data separate from secure data
    - **Screen Locks**
    - **Lockout -** Limited password attempts or Lost Mode
    - **Remote Wiping**
    - **Disabling Unused Features**
    - **Asset Tracking -** Where is the thing
    - **Inventory Control** - RFID tracking
- **BYOD Concerns**
    - Are the devices secure enough? Are users tracking out data?
    - **Acceptable Use Policy -** User responsibilities in return for privileges
    - **Privacy** - Not everything is private on company time
    - **User Acceptance** - User must agree to the rules and the privacy restrictions
    - **Data Ownership** - Org owns everything done internally, including emails
    - **Support Ownership** - Does IT have to help with BYOD?
    - **Architecture/Infrastructure -** What access do users have? What VLAN segmentation do they have?
    - **Forensics -** Can you see in-depth what users are using?
    - **Legal Concerns -** If a company doesn't set policy clearly, trouble.

    - **On-Boarding/Off-Boarding -** Employees must read BYOD policies and there must be rules for adding or removing devices
    - **On-board camera/video -** Should there be restrictions for security?
- **Mobile Device Management**
    - Many configuration managers like Microsoft ConfigMgr 2012 support mobile devices
    - **Patch Management**
    - **Antivirus Management**
    - **Application Control**
    - If devices don't meet regulations, they cannot connect.
    - **Application Security -**
        - Many apps have credential managers and caches which are risky
        - Many cameras have geo-tagging features which are also risky

Protecting Data

- **Data Categories**
    - **Data at Rest** - Any data stored on HDD, be that flashdrive, backups, or mobile phone
    - **Data in Transit** - Any data traveling over a network. Data Loss Prevention (DLP) analyze and detect sensitive data over a network, and you can also encrypt data using IPsec, SSH, or SFTP
    - **Data in Use -** Data in temporary memory, typically protected by the application using it
- **Protecting Data with Confidentiality**
    - ENCRYPT
    - Be careful to encrypt stored data, and keep it encrypted when its transmitted.
    - Other tools besides encryption are less secure; such as NTFS ACL permissions. If someone takes your NTFS hard-drive and puts it in another computer, they can give themselves access.
    - **Software Based Encryption**
        - Slower than hardware encryption, but secure with strong algorithms
        - **File- Level Encryption**
            - Linux uses **GNU privacy guard (GPG)** which is a command line tool used to encrypt and decrypt files with a password.
            - NTFS includes **Encrypting File System (EFS)** in windows explorer.
            - File/folder encryption allows you to add one more layer of security, even against Admin privileges
                - One risk to this is that if you copy to a file system that doesn't support NTFS encryption, it may decrypt the files before copying.
        - **Full Disk Encryption**

                - **TrueCrypt** is available to do this on linux and many OS
                - Requires a password and encrypts/decrypts drive on the fly
            - **Encrypting Database Content**
                - Oracle and Microsoft SQL and others allow you to encrypt specific elements, or the entire database.
                - You could, for example, not encrypt customer first names, but only their credit card and security code info. This saves processing power
    - **Hardware Based Encryption**
        - You can use a **Trusted Platform Module** or other hardware security module for higher performance encryption.
        - **TPM**
            - Chip in Mobo
            - Full disk encryption
            - Performs platform authentication (ensures drive not moved)
            - Includes Three keys
                - Endorsement key (burned into chip)
                - Endorsement key is *Rivest, Shamir, Adleman (RSA)*
                - Storage Root Key generates and protects other keys
                - Application Keys - derived from Storage Root key
            - To activate the TPM, you often use an application like bitlocker.
            - Without access to the TPM chip and authenticated credentials, the data remains secure
        - **Hardware Security Module**
            - A security device that can be added to a machine to manage, generate, and securely store keys.
            - High-performance HSM are connected to a network with TCP/IP
            - Smaller HSM are merely expansion cards plugged into a server
            - HSM performs very similar to TPM, but it is removable
- Data Leakage
    - Data Exfiltration - When data is transferred outside of an organization
    - **Data Loss Prevention (DLP)**
        - Examines data looking for unauthorized leaks
        - Can examine stored data, moving data, and data in use
        - **Data in Motion**
            - UTM devices include DLP to scan emails and files
            - A lot of data is labeled as Classified, confidential, private, and sensitive.
            - Once data is labelled, it can be inspected in transit and blocked if necessary
        - **Endpoint Protection**
            - Can include preventing flash drive usage or printing

Understanding SANS

- Might include Hard-drives, disks, tape, and optical media
- Often configured in fault-tolerant arrays for high-performance
- Robotic devices often assist in loading/unloading optical jukeboxes or tape libraries
- SANs often rely on high speed internal transfers
- **Virtual SANS** are a newer tech
- **Fibre Channel**
    - Speeds of up to 16 gigabits per second
    - Require special hardware and cabling
    - Expensive, albeit efficient
    - Some support copper, not just fiber
- **iSCSI - Internet Small Computer System Interface**
    - Transfers SCSCI commands over IP
    - Utilize existing network infrastructure
    - Allows SAN without specialized hardware
- **FCoE - Fibre Channel over Ethernet**
    - Uses FC commands, but transmits them over ethernet networks
    - FCoE encapsulated the commands within standard protocols
    - Allows ethernet LAN to act like Fibre Channel without the cost
- **Handling Big Data**
    - Data sets, like Amazons, that are too large for traditional tools to analyze them
    - Use many of the same tools, plus some special ones

Understanding Cloud Computing

- For example, Gmail is a SaaS (software as a service) cloud application
- Amazon's Elastic Compute Cloud (EC2) service provides elastic, on-demand servers to companies with variable traffic demands
- **Software as a Service**
    - Gmail, GDocs, etc
    - **Management as a Service (MaaS)**
        - Third party helps run IT resources, monitoring logs, etc
    - **Multi-Tenancy Architecture**
        - Like running multiple tabs in a web browser- one application instance for multiple users
        - Gdocs
    - **Single Tenancy Architecture**
        - Individual app instance for each user
- **Platform as a Service (PaaS)**
    - Preconfigured computing platform for customers
    - Also known as **Managed Hardware Solution**
    - Buying servers as web hosts

    - Can include OS, antivirus, spam protection, security, etc
        - Often includes up-to-date patches
    - You can manage the software you need for your uses, and let the rest of the server be handled by the company
- **Infrastructure as a Service**
    - The IaaS provider owns the equipment, the data center, and performs hardware maintenance, but the customer rents access to the equipment's functionality
    - Also known as **Self-Managed Solution**
    - Customer must configure the OS, software, etc
    - This means less hardware per company, so saves money on equipment, power, HVAC, and personnel
- **Public v Private Cloud**
    - Public is like Boxsync or Google Drive
    - Private is specific for a corporation
    - Hybrid clouds exist
- **Cloud Computing Risks**
    - You lose physical control of the data
    - You don't always even know where the data is
    - You don't control the security for your data, and cloud employees can be thieves themselves
    - "Only data you should put on a cloud is data you're willing to give away"

Malware and Social Engineering

Types of Malware

- **Viruses**
    - Attached to host application which must be run to activate virus
    - Tries to infect other application
    - May delete files, cause reboots, join computer to a botnet, or allow backdoors.
    - **Armored Virus**
        - The first step to dissecting a virus is to decompile it. Armored viruses make this difficult
        - **Complex Code**
            - It's unclear what the virus is trying to do because it runs so many weird loops
        - **Encryption**
            - Some compilers encrypt the code with the virus, so until this encryption is cracked, it can't be decompiled
        - **Hiding**
            - Some viruses confuse the AV as to where they're really located
- **Polymorphic Malware**

    - Virus that changes as it executes, sometimes into 1000 forms.
    - Hard to detect, especially if its encryption changes
- **Worm**
    - Self-replicating malware that travels without a host
    - Resides in memory and can ride transport protocols
    - Can replicate hundreds of times, draining network bandwidth
- **Logic Bomb**
    - Script that activates in response to an event like a date or a program launch
- **Backdoor**
    - Trojans commonly cause these
    - Provides another way to access a system
- **Trojans**
    - Look useful, but really suck
    - **Drive-By Downloads**
        - Attackers take over a website
        - Install a Trojan into the Web site's code
        - Attackers trick users into visiting the site
        - Web site tries to download the code
    - Fake antivirus called **RogueWare**
        - Runs a fake scan, and offers to fix fake issues for money
- **Botnet**
    - Computers in a botnet are called zombies
    - Bot herders manage these zombies to use their processing power and anonymity
- **Ransomware**
    - Pay to get your computer back or clean
- **Rootkit**
    - Stealthy bugger
    - Modify system processes and the registry, as well as system access files
    - Prevents antivirus from making calls to the OS that would detect it
        - Antivirus can scan memory to discover this
    - Safe mode helps get around this, but not always
- **Spyware**
    - Monitors stuff
    - Changing a user's home page, redirecting web browsers, installing software
    - **Privacy Invasive Software**
        - Tries to get the good data to drain your bank and steal your identity
    - Keyloggers
- **Adware**
    - Learn a users habits for ad-targetting
    - Pop ups!

Recognizing Common Attacks

- **Social Engineering**
    - Using social tactics to trick users into doing something unusual or revealing info
        - *Flattering and Conning*
        - *Assuming a Position of Authority*
        - *Encouraging Someone to Perform a Risky Action*
        - *Encouraging Someone to Reveal Sensitive Info*
        - *Impersonating Someone*
        - *Tailgating w/o credentials*
- **Shoulder Surfing**
    - Privacy screens, man
- **Hoaxes**
    - Trick people into deleting system programs, lololol
- **Tailgating and Mantraps**
- **Dumpster Diving**
    - Company directories are especially good treasure
    - Detailed company, personnel, or client info should be destroyed
- **Spam**
    - Often has malicious attachments or links
- **Phishing**
    - Like social engineering, but over email
    - Many people use fake accounts to look like your friends
    - Sometimes links are *beacons* and when you click that link, the tail-text tells that server that your email is active
    - **Spear Phishing**
        - More targeted at a user or user group
    - **Whaling**
        - Targeting CEOs and big wigs
        - Might install a keylogger
        - Might threaten subpoenas or other very specific things
- **Spim**
    - IM spam
- **Vishing**
    - VOIP spam
    - Spoofs caller ID and asks for sensitive info
- **Privilege Escalation**
    - Trying to get higher system privileges to access more stuff

Blocking Malware and Other Attacks

- **Anti-Malware on Mail Servers**
- **Anti-Malware on All Systems**

- **Boundaries or Firewalls**
- **Antivirus Software**
    - **Signature Based Detection**
        - Detects Known Patterns by checking against signature files
    - **Heuristic-Based Detection**
        - Watches for “viral behavior” rather than specific signatures
    - **Checking File Integrity**
        - If System file hashes change, you can tell they’ve been modified and there might be a virus
    - **Pop-up blockers**
    - **Spam Filters**
        - UTM contains spam filter, and Email server also scans for spam
        - User system also scans for spam
        - Don’t throw the baby out with the bathwater
    - **Anti-Spyware**
        - Specifically protects user info

Why Social Engineering Works

- **Authority**
    - **Impersonation**
    - **Whaling**
    - **Vishing**
    - If someone looks legit, users don’t want to question them.
- **Intimidation**
    - Bullying tactics, making things seem urgent and critical
    - Make the risk of non-compliance high
- **Consensus/Social Proof**
    - Fake testimonials/reviews
    - Fake popularity
- **Scarcity**
    - Limited quantities imply urgency
- **Urgency**
    - Give people limited time to respond to panic them
- **Familiarity/Likability**
- **Trust**

Identifying Advanced Attacks

Comparing Common Attacks

- **Spoofing**
    - Digital Impersonation
    - Email spoofing, for example, is when you make the “from” address in an email appear as if it were from someone else
- **Dos v DDoS**
    - How many computers are attacking a target?
    - The goal is to get the target to use up enough resources that it can’t service real users
    - Indicated by sustained, abnormally high traffic
    - **Smurf Attacks**
        - Spoofs the source address of a directed broadcast ping to flood a victim with ping replies
        - Smurf attack sends a ping as a broadcast but pretends the victim was the source
        - This makes all the recipients of the original ping ping back against the victim
        - Most routers block directed broadcasts by default - this protects them from becoming part of an amplifying network
    - **SYN Flood Attacks**
        - Utilize the TCP handshake by sending swarms of SYN, but never sending the final ACK
        - Most servers will stop accepting new connections until the half-connections are settled
        - Some servers just crash
        - **Flood Guards**
            - Use a variety of means to prevent floods
            - Can detect the IP of the attacker and block them
            - Can reduce the wait time for the ACK packet
            - Etc
- **Xmas Attacks**
    - Port scan used to get details about an OS
    - It sends bits in the packet header of the TCP port scan that resemble christmas lights
    - This gives it info about how the system responds and what OS it is.
    - It’s more for recon than anything
    - Many IDS and IPS can detect this
- **Man-in-the-Middle Attacks MITM**

    - Active interception or eavesdropping
    - Sits in the middle and takes both streams of traffic, and can send on malicious code
    - Kerberos' mutual authentication can thwart it
- **Replay Attacks**
    - Steal all the authentication data transferred between two clients, then try to send out that authentication data again to pretend to be one of the two
    - Timestamps and sequence numbers thwart this
    - Kerberos uses timestamps
- **Password Attacks**
    - Attempts to discover or bypass passwords
    - **Online Password Attack**
        - Attempt to discover password from online system or guess
    - **Offline Password Attack**
        - Capture database or packet and try to decrypt it
        - WPA cracking
    - **Brute Force Attack**
        - Get yoself some complex passwords with account lockout policies
    - **Dictionary Attack**
        - Brute forces all the easy words
    - **Password Hash**
        - Attack the stored hash of a password rather than the password
        - Websites like MD5 Online can reverse these hashes
    - **Birthday Attacks**
        - Named after birthday paradox in probability theory
        - Works on easy hashes where you just come up with a password that produces the same hash
        - **SHA-2 (Secure Hash Algorithm 2)** used 512 bits (compared to MD5's 128) so its much harder to match
    - **Rainbow Table Attacks**
        - Rather than hashing every guess individually, you use large tables of preconfigured hashes to check the password hash against
        - **Salting** passwords makes this more difficult, wherein two random digits are added to a password to make the hash more complex
            - Bcrypt and Password-Based Key Deviation Function 2 (PBKDF2) both use salting to increase the complexity of passwords.
    - **Hybrid Attacks**
        - Try out multiple things!
- **DNS Attacks**
    - **DNS Poisoning**
        - Modifies or corrupts DNS results
        - If someone typed google.com, they may end up somewhere else

        - DNSSEC (DN System Security Extensions) protects DNS records and prevents poisoning
    - **Pharming Attacks**
        - Tries to corrupt DNS server or DNS client to redirect users to the wrong site
        - On clients, these modify the hosts file to change the default entry of specific sites
        - This can be a prank, but can really cause trouble
- **Arp Poisoning Attacks**
    - Misleads computers or switches about the MAC address of a system
    - ARP sends requests and replies, and its easy to spoof a reply
    - **ARP MitM Attack**
        - Spoof the ARP cache on a switch so it sends data to the attacker, who saves it and forwards it along like usual
    - **ARP DoS Attack**
        - Spoof so everyone caches a bogus default gateway MAC address
        - Nobody can communicate properly
- **Typo Squatting/URL Hijacking**
    - Similar domain names that people often misspell
- **Watering Hole Attacks**
    - Figures out where employees of an org spend their web time and then infects those locales or tries to redirect them to a malicious site
    - Often to install RATs to get access to the org
- **Zero-Day Attacks**
    - Exploits undocumented vulnerability
    - Serious until patched
    - Relevancy depends on how known it is
- **Web Browser Concerns**
    - **Malicious Add-Ons**
    - **Cookies and Attachments**
        - Normally only the site that makes a cookie can read it, but cross-site scripting can allow attackes to steal personal info from them
    - **Session Hijacking**
        - You can also use cookies to session hijack
    - **Flash Cookies and LSOs**
        - Cookie made by Adobe Flash Player, also known as **Local Shared Objects**
        - Flash cookies can be stored in special places and aren't always cleared with the rest of the cookies
        - They track data discretely which has led to a lot of lawsuits
    - **Arbitrary Code Execution/Remote Code Execution**
        - Allows attackers to run specific code on a system without user consent
        - Software bugs often allow this

- **Header Manipulation Attacks**
    - Manipulate the flags in TCP/IP headers to change behavior, or change session ID within the packet
    - This session ID can allow the attacker to steal your sign-in and access your stuff

Understanding Secure Coding Concepts

- **Input Validation**
    - Checking data before using it
    - Can either clear out malicious data or reject the whole submission
    - **Verifying Proper Characters -** Only the right characters for that field, such as only numbers in a US zip
    - **Implementing boundary or range checking** - if max purchase is three, can only submit 3 or less
    - **Blocking HTML code**
    - **Preventing the use of certain characters** - such as dash, apostrophe, and equal sign
- **Client-Side and Server-Side Input Validation**
    - Client side is quicker, but vulnerable
    - Server side takes longer, but is secure
    - If you disable javascript, you can often get through client side validation in a web browser
- **Avoiding Race Conditions**
    - Don't let two parts of an app, or two apps, attempt to access a single resource at once.
    - This can cause obvious conflicts
- **Error and Exception Handling**
    - Provide user feedback when there's an error
        - **Errors to users should be general** don't give an attacker too much info
        - **Detailed Info should be logged -** Debug info goes to support team

Identifying Application Attacks

- **Web Servers**
    - **Apache -** Free Unix/Linux/Windows
    - **Internet Information Services (IIS)** - Microsoft web server and free with windows server products
- **Buffer Overflows and Buffer Overflow Attacks**
    - When an app receives more or different input than it expects
    - Can expose system memory that should be protected
    - A skilled attacker can use this exposed vulnerability to rewrite their own malicious code into system memory
        - This relies on some educated guesses normally
        - **NOP (No-op)** commands make this easier.

                - Many intel processors use hexadecimal 90 as a NOP command, so a string of x90 characters is a NOP sled
                - When the processor comes across a string of x90 NOP, it just jumps to the next memory location, which the attacker has filled with malicious code
                - *BufferOverflowData:NOPs:Malicious Code*
- **Integer Overflow**
    - By knowing what bitrate the server stores numbers, you know the upper limits of numbers it can store. You can push it above that limit to make it throw an error
- **Injection Attacks**
    - **SQL Queries and SQL Injection Attacks**
        - **Structured Query Language**
        - **SQL Queries**
            - Translates user input into a clear database call and returns the selected info
        - **SQL Injection Attacks**
            - By understanding SQL syntax, you can often inject several extra commands into this search to get the database to return info that its not supposed to
            - Error handling will prevent these injections if configured properly
                - These errors can often give more info about the kind of database being used
            - You can also use logic to tell the computer to return all results '1' = '1'
        - **Protecting Against SQL Attacks**
            - Treat the whole damn user entry as a string lol
        - **XML Injection**
            - Pretty similar, but in XML
        - **NoSQL v SQL Databases**
            - Also include documents, graphs, and key-value pairs
            - Allows developers more storage flexibility
            - Uses **Unstructured Query Language (UQL)**
                - Attackers can learn this, though it may vary with vendor
    - **Cross-Site Scripting (XSS)**
        - Embed malicious HTML or javascript code into an email or website error
        - Someone embedded code on twitter that infected computers when people looked at the tweet
    - **Cross-Site Request Forgery (XSRF)**
        - Adding tails to URLs that automatically make people perform actions
        - Combined with auto-logon cookies, this is dangerous
        - Making users re-authenticate before making changes helps
    - **Directory Traversal/Command Injection**
        - Injecting full system commands and pathways into web page forms

    - **LDAP Injection**
    - **Transitive Access and Client-Side Attacks**
        - Utilizes transitive trust properties and injections to piggyback connections and access even MORE data from an initial SQL injection
    - **Fuzzing**
        - Using a program to send random data to an app
        - Might crash or provide unexpected results, but may reveal a vulnerability

Managing Risk

- **Threats and Threat Vectors**
    - **Natural Threats** - “I AM A HURRICANE”
    - **Malicious Human Threats -** “Muahahahaa”
    - **Accidental Human Threats** - “Whoops!”
    - **Environmental Threats** - Long term power failure leading to chemical spills, etc
    - **Malicious Insider Threat**
        - Someone with legit access to internal resources and seeks to exploit them
        - Hence, least privilege.
- **Threat Assessments**
    - How likely are specific things, and what will cause the most harm?
    - **Vulnerabilities**
        - **Lack of Updates**
        - **Default Configurations**
        - **Lack of Malware Protection**
        - **Lack of Firewalls**
        - **Lack of Organizational Policies**
        - Just because it hasn’t been attacked, doesn’t mean it’s not vulnerable. Audit regularly and look for new things each time.
- **Risk Management**
    - **Risk Avoidance** - Don’t participate in risky activity or opt not to provide a risky service
        - If something requires you to open several unsecure ports, ask yourself if its worth it
    - **Risk Transference** - Can you share the risk with another entity, or put it on their lap?
        - Insurance, outsourcing, etc
    - **Risk Acceptance**
        - Would it be more expensive to protect the device than the device is worth?
        - What’s the real cost of a loss, vs the cost of the protection
    - **Risk Mitigation**

        - Reduce the risk with up-to-date tech
    - **Risk Deterrence**
        - Security controls make it harder to attack you, and make you a less appealing target
- **Risk Assessment**
    - Identify assets and their values
    - Identify threats and vulnerabilities to the highest value assets
    - Set recommendation for what controls will mitigate those risks
    - These assessments should change as conditions do
    - **Quantitative Risk Assessment**
        - Lists the specific monetary value of assets vs specific cost of mitigating controls
        - **Single Loss Expectancy (SLE)**
            - Cost of a single loss
        - **Annual Rate of Occurrence (ARO)**
            - How often will that loss occur in a year?
        - **Annual Loss Expectancy (ALE)**
            - SLExARO=ALE
        - Compare the ALE to the Annual cost of mitigating controls. How much do you spend to save how much more?
        - Qualitative risk might say that even though it costs a little more for the protection, its worth it (for savings in privacy, company's status, etc)
    - **Qualitative Risk Assessment**
        - Judge based on probability and impact
        - Probability is obvious
        - Impact includes loss of confidentiality, integrity, or availability of system data
        - You might use a host of experts in a focus group to determine the risk and impact
        - You can assign numbers on a 1-10 scale to make it easier to assess risk
    - **Documenting the Assessment**
        - File a report including the numerical risk values and recommended solutions
        - Management can review these reports to make final decisions
        - A final report can document what risks were accepted vs. mitigated
        - DO NOT let an attacker get these reports
    - **Metrics to Assess Risk**
        - **Mean Time Between Failure (MTBF) -** System's reliability in hours. Lists average hours between failures.
        - **Mean Time To Failure (MTTF) -** Length of time a device can be in service before it fails. Primarily indicates a device that cannot be repaired.
        - **Mean Time To Recover (MTTR) -** Average length of time to restore a system

Checking for Vulnerabilities

Anatomy of an Attack

- Recon on the larger target, then honing in for details (fingerprinting) of individual targets.
- **Identifying IP Address of Targets**
  - Starts with Geographic Location
  - Use ICMP sweep to identify operational systems in a region using **Ping Scanner**
  - Its possible to block ICMP at a firewall to prevent Ping Scanners
- **Identifying Open Ports with a Port Scanner**
  - By noting open ports, you know what protocols and applications are likely in use
  - Advanced Scanners send further queries to some known ports to make sure a protocol is running and find out more info about the system
  - For instance, HTTP can tell you whether its on Apache or IIS
  - Nmap, Netcat, and Nessus all include port scanning abilities, and sec professionals use them to perform self-analysis
- **Fingerprint System**
  - Sends specific protocol queries to identify what OS is running based on details of query responses
  - **Banner Grabbing**
    - Gain info about a service running on an open port
    - For example, Telnet into a website (port 80) and send an HTTP request, it will shoot back information like OS, server type/version, Content type, time
- **Identifying Vulnerabilities**
  - Once you know the fingerprint details, you get experts on the specific infrastructure you're trying to attack.
  - You can test input validation, default accounts, and use vulnerability scanners to identify current patches
- **Attack**
  - Once everything is planned, attackers try to move quickly so nothing can be patched or updated, and that its harder to detect them. They'll smash and grab, trying to get as much as possible before they're blocked out
- **APT - Advanced Persistent Threats** are very real, and can be government funded, well-organized, and resourceful. They have the skills and patience to break through most defenses given enough time.
  - This is why it's important to segment traffic and data, limit user permissions, and train people to avoid malware. Attacks are very

reasonably possible, so you must limit the damage that can be caused by a single attack.

Vulnerability Assessment

- Use vulnerability scanners, port scanners, etc
- Identify assets and risks
- Prioritize what mitigating factors you'll use
- **Vulnerability Scanning**
    - **Identifies Vulnerabilities**
    - **Identifies Misconfigurations**
        - Open Ports
        - Weak Passwords
        - Default accounts and pws
        - Sensitive Data - DLP
        - Security and Configuration Errors
    - **Passively Tests Security Controls**
        - Identifies only, does not exploit
        - Does not interfere with normal operations until an admin can assess
    - **Identifies Lack of Security Controls**
        - Lack of patches or antivirus
- **Other Assessments**
    - Checking for tailgating spots, social engineering risks, etc
    - See if employees are dumb enough to give out passwords
    - **Baseline Reporting**
    - **Code Review**
    - **Attack Surface Review**
    - **Architecture Review**
        - Is a database accidently in a DMZ? Add a firewall
    - **Design Review**
        - How do apps interact? What's the building layout?
- **Credentialed v Noncredentialed**
    - Scanners can run with a variety of credentials to see the risk at different levels of user access
- **Penetration Testing**
    - Tries to exploit vulnerabilities to detect impact of an attack
    - You can also use this to see how a company will respond in case of an emergency
    - *Verify a Threat*
    - *Bypass Security Controls*
    - *Actively Test Security Controls*
    - *Exploit Vulnerabilities*

    - A fake attacker could try an SQL injection to get credentials, then use those credentials to break in further and test his luck
    - This can disrupt daily ops, but is very informative
- **White, Gray, Black Box testing**
    - **Black Box** - Testers have 0 knowledge of environment just like an attacker
    - **White Box** - Full knowledge of environment and documentation
    - **Gray Box** - Testers kind of know whats going on
- **Obtaining Consent**
    - Don't pentest without consent in *writing*.
    - Use a "rules of engagement" doc
- **Passive v Active Tools**
    - Vuln scanning is PASSIVE
    - Pentesting is ACTIVE
- **Continuous Monitoring**
    - CONSTANT VIGILANCE

Identifying Security Tools

- **Sniffing with a Protocol Analyzer**
    - Captures and analyzes packets sent over a network
    - Can be used by admins or attackers
    - Any open wiring or switch could be vulnerable
    - Wireshark is a free protocol analyzer you can use
    - Analyzing packets is tedious, but full of info
    - An NIC must use **Promiscuous Mode** to capture all traffic- it allows it receive traffic without being the designated IP
- **Routine Audits**
    - Double checks to ensure everything is at baseline and rules are being followed
- **User Reviews**
    - Ensure least privilege is being followed and users aren't accessing what they shouldn't
    - Privilege Creep and Inactive Accounts are both threats
    - If someone keeps transferring departments and getting new access, does anyone ever clear the old access?
    - Role-based privileges make this easier to manage
- **Monitoring Events with Logs**
    - Don't waste disk space, log whats important.
    - **Operating System Event Logs**
        - **Security Log**
            - Includes log ons/offs and resource access
            - You can configure auditing to denote what should be logged
        - **Application**
            - Records events logged by apps or errors

        - **System**
            - Starts, shuts down, services starting or stopping, drivers loading or failing
    - **Firewall and Router Access Logs**
        - Packet sources and destinations including IPs, ports, MAC addresses
        - **Antivirus Logs**
        - **Application Logs**
        - **Performance Logs**
    - **Reviewing Logs**
        - NetIQ has a suite of apps that will review logs on multiple servers and computers
        - Notes ‘of interest’ events and sends up an alert
        - Likely centralizes logs beyond individual hosts

Preparing for Business Continuity

Adding Redundancy

- For instance
    - Disk Redundancy with RAID
    - Server Redundancy with Failover Clusters
    - Power Redundancy with UPS/Generator
    - Site Redundancy with hot/cold/warm sites
- **Identify Single Point of Failure**
    - If it breaks, will something take its place, or does everything go down?
    - **Disk** - Will a system crash without this disk? Will the data be lost forever?
    - **Server** - Will the service stop if this goes down? What else relies on that service?
    - **Power** - If there’s a power outage, what takes its place?
- **See RAID above**
- **Server Redundancy**
    - 99.999% availability = 5 nines.
    - Less than six minutes of downtime a year
    - Expensive, but could be justified depending on costs of downtime.
    - **Failover Clusters**
        - Two or more servers as nodes in a cluster
        - At least one inactive node
        - If active node fails, inactive node takes over.
    - **Load Balancers for High Availability**
        - Distributes traffic and data loads across system devices
        - Allows for scalability
        - Load balancing also detects failed devices
- **Power Redundancy**

    - **UPS** - Provides power until any one of three goals
        - System should have enough time to shut down
        - Generators have enough time to power up and stabilize
        - Commercial Power returns
    - **Generators**
        - Expensive to run, but cheaper than failure
        - Should be able to run for a long time
- **Protecting Data with Backups**
    - Ensure that when data is lost or corrupted, it can be retrieved
    - Redundancy does not remove the need for backups
    - **Tapes**
        - **Full Backup**
        - **Differential Backup** - backs up all changes since full backup
        - **Incremental Backup** - backs up all changes since last differential or incremental backup
            - Each incremental tape needs to be kept because the backups are not cumulative
        - Which setup you go with depends on maintenance time throughout the week and loss acceptance
        - Restorations take longer with smaller incremental backups
    - Its important to test backups, because it sucks if they fail
    - **Protecting Backups**
        - Use clear labelling in storage and physical security to protect them from theft
        - Protect it well if its being moved from one location to another.
        - Destroy backups when they're no longer needed.
- **Backup Policies and Plans**
    - **Identify Data to Backup**
    - **Requires off-site backups**
    - **Requires Labeling Media**
    - **Mandates Testing of Backups**
    - **Identifies Retention Requirements**
        - Note related laws on how long data needs to be stored
        - Also note how much data you want available if you go to court lol
    - **Designate Frequency of Backups**
    - **Protects Backups**
    - **Identifies Acceptable Disposal Methods**

Comparing Business Continuity Elements

- Disasters can come from
    - Fires
    - Attacks

- Power Outages
- Data loss
- Hardware/software Failurewithdrawing account funds need to be always live
- A business must decide:
    - Natural disasters
- **Business Continuity Planning (BCP)** follows these steps
    - Complete a Business Impact Analysis
    - Develop Recovery Strategies
    - Develop Recovery Plans
    - Test Recovery Plans
    - Update Plans
- **Business Impact Analysis (BIA)**
    - Some systems can be delayed, like loan processing, but accessing and
    - What are critical systems and functions?
    - Are there dependencies related to those systems?
    - What is the maximum downtime of those systems?
    - What scenarios would most likely affect those systems?
    - What is the potential loss from these scenarios?
- You might decide that your maximum downtime is five hours, so now you need to plan how you would recover from any disaster in less than that time.
- You might recognize that losing data from a secure server could cost you millions- so now you know you should be willing to spend a lot to make sure you never lose data from it.
- **Recovery Time Objective (RTO)**
    - Max duration systems can be down.
    - Might have different RTOs for different systems
- **Recovery Point Objective (RPO)**
    - How often you need to backup data in order to ensure you have acceptable data loss.
- **Continuity of Operations Planning (COOP)**
    - Setting up an alternate location that can run things if things go nuts, like in a hurricane.
    - **Hot site** - when you need ops in 60 minutes.
    - **Cold site -** when you have a few days.
    - **Mobile site** - set up and tear down for when a company doesn't want a permanent alternate site. Could be in a semi trailer.
    - **Mirrored site**- 100% identical to the primary location including real-time data transfer.
- **Disaster Recovery Plans (DRP)**
    - Includes a hierarchical list of critical systems indicating the order to restore systems
        - **Activate Disaster Recovery Plan**
        - **Implement Contingencies**

            - Backup sites/systems, etc
        - **Recover Critical Systems**
        - **Test Recovered Systems**
        - **Document and Review**
    - **Planning for Communications**
        - **War Room -** conference room where people get their updates and report in
        - You must be able to communicate with these people even if cell lines are down:
            - **Disaster Response Team Members**
            - **Employees**
            - **Customers**
            - **Suppliers**
            - **Media**
                - Get a PR agency, don't let a tech talk to the press
            - **Regulatory Agencies**
    - **IT Contingency Planning**
        - Focused only on IT, rather than full business
    - **Succession Planning**
        - Who takes over when…?
        - Who has say when…?
        - Someone needs authority, but it can't be just anyone
    - **BCP and DRP Testing**
        - Tabletop and functional exercises
            - **Backups**
            - **Server Restoration**
            - **Server Redundancy**
            - **Alternate Sites**
        - **Testing Controls**
            - Try turning stuff off and see what breaks or what takes over
        - **Escape Plans, Escape Routes, Drills**
- **Implementing Environmental Controls**
    - **Heating, Ventilation and AC**
        - If HVAC fails, it can fry your servers
        - Sometimes its worth shutting down the systems if the HVAC can't keep up with the load or fails
    - **Hot and Cold Aisles**
        - Some aisles exhale hot air, some pull in cold
        - Make the backs of two racks face each other
    - **HVAC and Fire**
        - HVAC often have fire alarm systems because if they pump oxygen into a fire, the fire goes nuts, but alternately a well designed HVAC can fight the fire with dampers

- **Fail-safe v Fail-open**
    - Does it fail to be most secure, or most safe for people?
    - Doors should fail open, firewalls should fail-safe.
- **Fire Suppression**
    - **Remove the Heat** with chemical fire extinguishers
    - **Remove the oxygen** with CO2
    - **Remove the Fuel**
    - **Disrupt the chain reaction** with chemicals
    - Four Classes of Fires
        - **Class A - Ordinary Combustibles -** wood, paper, cloth, rubber, trash, and plastic
        - **Class B - Flammable Liquids** - Gasoline, propane, solvents, oil, paint, etc
        - **Class C - Electrical Equipment** - Computers, wiring, etc. Don't throw water on it.
        - **Class D - Combustible Metals** - magnesium, lithium, titanium, sodium.
- **Environmental Monitoring**
    - Includes Temp/Humidity sensors
    - **Shielding -** protects from EMI
        - If data radiates outside a cable through EMI, it can be stolen
        - **Shielding Cables**
        - **Protected Distribution of Cabling**
            - Planning where you route cables so an attacker can't throw on an RJ45 end or Fiber end and hack your shit
        - **Faraday Cages**
            - Room that prevents signal radiation past the barrier

Understanding Cryptography Take this quiz again for review - 10

Basics

- **Integrity**
- **Confidentiality**
    - **Encryption Basics**
        - **Symmetric Encryption**
            - Same key to encrypt and decrypt data
        - **Asymmetric Encryption**
            - Two keys, public and private, created to match.
            - Anything encrypted with the public key can only be decrypted by the private key

        - Anything encrypted with the private key can only be decrypted by the public
    - **Stream Ciphers** encrypt data one bit at a time.
    - **Block ciphers** encrypt data in blocks
    - **Steganography** provides a level of confidentiality by hiding data within other files
- **Authentication** validates identity
- **Non-repudiation** refers to the ability to ensure that a party cannot deny the integrity of their own signature
- **Digital Signature** provide authentication, nonrepudiation, and integrity
    - A digital signature in an email is a hash of the email encrypted with the sender's private key
    - Only the sender's public key can decrypt the hash which verifies it was sent by the sender's private key

Hashing

- An algorithm run on data that can be used again later to confirm that data hasn't been changed, without having to parse the entire data
- **MD5 - Message Digest 5**
    - Produces 128 bit hash in hexadecimal
    - Often used to verify files and downloads
    - Website can display the hash, and then you can test the hash after download to make sure its the same
- **SHA - Secure Hash Algorithm**
    - **SHA-0** unused
    - **SHA-1** creates 160 bit hashes similar to MD5
    - **SHA-2** includes **SHA-224, SHA-256, SHA-384, and SHA-512**
    - **SHA-3** uses a different method than SHA-2. Supports 224, 256, 384, and 512 bits as well.
    - Some HIDS and antivirus capture hashes of files when they first scan through, and then later they capture new hashes to compare. If any hashes are different, there is a possibility of malware.
- **HMAC** - **Hash-based Message Authentication Code**
    - Such as **HMAC-MD5 and HMAC-SHA1**
    - Uses a standard hash string of bits in conjunction with a secret key only known by the sender and receiver.
    - Creates the hash with the basic bits, then calculates on top of that with the secret key.
    - Not only does it protect integrity, but it also adds authenticity by ensuring that the message could only come from the verifiable sender
    - IPsec and TLS often use HMAC
- **Hashing**

    - Most applications perform hashes automatically, but programs like md5sum.exe will allow you to run them manually.
    - Passwords are often stored in hashes for security reasons
    - Now if an attacker can change a message, they could also change a hash, and that's why HMAC is more secure, because the hacker can't properly fake that hash.
- **Other Hash Algorithms**
    - **RIPEMD - RACE Integrity Primitives Evaluation Message Digest**
        - Creates 128, 160, 256, and 320 bit hashes.
    - **LANMAN and NTLM**
        - Older Microsoft hashing algorithms for passwords
        - **LANMAN** Lan Manager
            - Windows 95, 98, and ME
            - Can't handle passwords longer than 14 characters
            - Easy-to-crack because of the way it fills with trailing spaces and hashes two 7 character codes
            - 7 character hashes too easy yo
        - **NTLM - NT LAN Manager**
            - Improved LANMAN
            - NTLMv1 uses an MD4 hash and occasionally LANMAN, so its useless
            - NTLMv2 uses an MD5 hash which is hard af to crack
                - Before Vista, many systems leave LANMAN enabled by default for backwards compatibility, which is baaaad.
            - The reason for 15 character passwords is to prevent LANMAN from being used

Encryption

- Two main parts to encryption
    - **Algorithm**
        - Always the same
    - **Key**
        - Provides variability for encryption, goes into the algorithm
        - Either private or changed often
- **Symmetric Encryption**
    - Same key to encrypt and decrypt
    - Also called **Secret Key** or **Session Key** encryption
    - **AES** uses 128 bit, 192, or 256 bit keys
    - Keys can be changed whenever a session is authenticated or re-authenticated
        - This is how RADIUS works
    - **Block v Stream Ciphers**
        - Stream are more efficient when… streaming

        - Block are more efficient when size of data is known.
        - WEPs vulnerability came from reusing keys on a stream cipher, so an attacker just had to be patient.
    - **AES**
        - Strong symmetric block cipher
        - **National Institute of Standards and Technology (NIST)** adopted AES from Rijndael encryption algorithm.
        - **AES** uses 128 bit, 192, or 256 bit keys
        - **Fast, efficient, and strong**. Best of the best.
    - **DES**
        - Symmetric Block Cipher used since the 70s. 64 bit blocks with a key of 56 bits, which is chump work nowadays.
    - **3DES**
        - DES improvement. Encrypts in three passes.
        - Strong, but resource intensive.
        - Useful when AES isn't supported.
    - **RC4**
        - Used in WEP, but not to blame for WEP's insecurity.
        - Recommended in SSL and TLS for encrypting HTTPS
        - Speculation that NSA can crack RC4
        - AES is still better, haha.
        - Stream Cipher
    - **Blowfish and Twofish**
        - 64-bit blocks and keys from 32 to 448 bits.
        - Faster than AES in some situations.
            - **Twofish**
                - 128 bit blocks
                - 128, 192, or 256 bit keys.
                - Almost used for AES, but Rjindael beat it.
    - **One-time Pad**
        - One of the most secure algorithms, but very labor intensive.
        - Each key is on a page of a pad, and destroyed after use.
        - Tokens and fobs are like digital successors to these.

Algorithm	Type	Method	Key Size
AES	Symmetric encryption	128-bit block cipher	128-, 192-, or 256-bit key
DES	Symmetric encryption	64-bit block cipher	56-bit key
3DES	Symmetric encryption	64-bit block cipher	56-, 112-, or 168-bit key
Blowfish	Symmetric encryption	64-bit block cipher	32- to 448-bit key
Twofish	Symmetric encryption	128-bit block cipher	128-, 192-, or 256-bit key
RC4	Symmetric encryption	Stream cipher	40- to 2,048-bit key

- Asymmetric encryption
    - Private keys are never shared
    - Public keys are freely shared within a certificate
    - More resource intensive than symmetric encryption.
    - Often asymmetric encryption is only used to privately share a symmetric key
    - **Certificates**
        - **Certificate Authorities (CA)** issue and manage certificates.
        - **Serial Number** - unique to certificate, CA uses to validate, and if it's revoked, a **CRL - Certificate Revocation List** will update that
        - **Issuer**
        - **Validity Dates**
        - **Subject**
        - **Public Key**
        - **Usage**
    - **RSA - Rivest, Shamir, Adleman**
        - Asymmetric encryption that’s widely used
        - Email often uses RSA to share a symmetric key
        - **TPM and HSM** both store RSA keys
        - Supports a minimum of 1,024-bit keys, and often 2048 or 4096 are recommended
    - **Static v Ephemeral Keys**
        - Static keys are semi permanent
        - Ephemeral keys are recreated each session
        - RSA uses static keys that are valid for the lifetime of a certificate, often a year
        - Diffie-Hellman can use either static or ephemeral keys.
        - **Perfect Forward Secrecy** is an important characteristic for ephemeral keys, and it's that the public keys are random, not deterministic.
    - **Elliptic Curve Cryptography**
        - Often used with wireless devices because it requires less processing power to encrypt, but is still hard to crack.
        - Even the NSA endorsed ECC

    - **Diffie-Hellman**
        - Means for sharing symmetric keys securely
        - **DHE** and **ECDHE** both use ephemeral keys.
- **Steganography**
    - Hiding data in other data.
    - Hide data by manipulating bits without affecting the final product.
    - Hide data in the white space of a file. Gifs and Jpegs save in blocks, so can be modified without changing the file size.
    - Steganalysis uses hashing to detect changes.
- **Quantum Cryptography**
    - exploiting quantum mechanical properties, such as Heisenberg's Uncertainty Principle, to perform cryptographic tasks
    - If alice and bob try to establish a key and eve tries to gain information about this, key establishment will fail.

Using Cryptographic Protocols

- **Basics**
    - Email Digital Signatures
        - Sender's *private key* encrypts.
        - Sender's *public key* decrypts.
    - Email Encryption
        - The *recipient's public key* encrypts.
        - The *recipient's private key* decrypts.
    - Web Site encryption
        - The *web site's public key* encrypts (symmetric)
        - The *web site's private key* decrypts (symmetric)
        - The *symmetric key* encrypts data in the web session.
    - Often assymetric encryption is used to securely share symmetric keys.
    - Just knowing that a private key is encrypting is enough to know its being used as a digital signature.
- **Protecting Email**
    - To send a digital sig on an email, you click a button which hashes the message
    - App uses her private key and encrypts the hash
    - App sends the hash and message to receiver
    - Receiver's system uses Lisa's public key from either the network, or an attached certificate
    - Email decrypts the hash with lisa's public key
    - App calculates a hash on the message
    - Compares decrypted hash with calculated hash
- **Encrypting Email**
    - **With Only Assymetric**
        - Lisa retrieves Bart's certificate and public key

        - Lisa encrypts the email with his public key
        - Lisa sends the email
        - Bart uses his private key to decrypt
    - **With Both**
        - Lisa picks a symmetric key to encrypt her email, let's say 51
        - Lisa encrypts her email with that key.
        - Lisa gets bart's certificate to take his public key
        - Lisa uses bart's public key to encrypt the symmetric key of 51
        - Lisa sends the encrypted email and encrypted symmetric key to bart
        - Bart decrypts the symmetric key of 51 with his private key, and then uses 51 to decrypt the email
    - **S/MIME - Secure/Multipurpose Internet Mail Extension**
        - Very popular email standard for signing/encryption
        - Uses RSA for asymmetric, and AES for symmetric
        - Requires PKI to distribute and manage certs
    - **PGP - Pretty Good Privacy**
        - OpenPGP is a PGP standard that circumvents licensing
        - GNU Privacy Guard is free and based on OpenPGP
        - PGP uses asymmetric and symmetric, and some versions follow S/MIME
- **Transport Encryption**
    - **SSH** - for SFTP, SCP, and Telnet
    - **HTTPS** - uses SSL or TLS over port 443
    - **IPsec**
        - Can encrypt data in tunnel mode with VPNs such as L2TP/IPsec.
        - Uses Authentication Header through HMAC which not only hashes, but uses a private key encryption on top of the hash.
        - Can use **Encapsulating Security Payload (ESP) to provide confidentiality with AES or 3DE**S. Protocol ID 50.
        - In ESP packet, there's an additional IP header over the whole packet, which doesn't allow attackers to see anything more than just that this is an ESP packet.
        - Mandates HMAC, AES/3DES
    - **SSL**
        - HTTPS and FTPS both utilize to encrypt web traffic
        - Certificate based authentication
        - Both asymmetric and symmetric keys
        - Netscape made SSLv3, but when netscape waned, nobody maintained SSL properly. TLS fills this gap.
    - **TLS**
        - Replaces SSL, and TLS 1.0 is actually SSL 3.1.
        - Cert based authentication
        - Asymmetric and symmetric encryption

        - EAP-TLS is the most secure version of EAP (802.1x servers that authenticate users signing into a network) because it requires certs on both host and server.
- **Cipher Suites**
    - Cipher suites are how two systems know which sets of cryptographic algorithms they're going to use together.
    - These provide Encryption, Authentication, and Integrity solutions.
    - There are over 200 named cipher suites that identify:
        - **Protocol**
        - **Key Exchange MEthod**
        - **Authentication**
        - **Encryption**
        - **Integrity**
    - You can enable or disable cipher suite options in a system
- **Strong Versus Weak Ciphers**
    - Only use the strength you need to limit resource drain, but also don't go too weak.
- **Encrypting HTTPS traffic with SSL or TLS**
    - Client requests secure session
    - Server sends its certificate including its public key
    - The client creates a symmetric key and and encrypts it with the servers public key
    - The client sends the encrypted symmetric key to the server
    - The server decrypts the symmetric key using its private key
    - All of the session data from thereon is encrypted with the symmetric key
- **Key Stretching**
    - Technique used to increase the strength of stored passwords
    - **Bcrypt**
        - Based on blowfish.
        - Salts passwords by adding extra bits before encrypting with blowfish
    - **PBKDF2**
        - WPA2 and iOS use this. Salts with at least 64 bits
- **In-band v Out-of-Band Key Exchange**
    - In-band means you send keys and data in the same channel
    - Out-of-band means you share the key outside of the channel that you share data

Exploring PKI Concepts

- Allows two entities to communicate securely without previous contact
- **Certificate Authority**
    - Issues, manages, validates, and revokes certificates.
    - Large companies like Verisign, which services Amazon, or small service.
    - CA's must be trusted, because they make money by selling certs.

- **Certificate Trust Paths and Trust Models**
    - CAs are trusted by placing their root certificate into a trusted root CA store.
    - CAs have to negotiate with web browsers to get their certificates added into that browset
    - **Hierarchical Trust Model**
        - Root CA issues intermediate CAs
        - Intermediate CAs issue certs to child CAs
        - Child CAs issue certs to devices or users
    - **Self-Signed Certs**
        - You can create your own CA and use it internally in your company, but if a third party tries to connect, their web browser will reject it
        - In order to make computers trust it, you need to copy the root certificate to each computer that will be connecting to the CA
    - **Wildcard Certificates**
        - Certificate good for additional level of domains such as store.google.com or docs.google.com.
- **Registration**
    - Use a program like SSL to make yourself a public/private key.
    - Create a **Certificate Signing Request (CSR)** for the cert, including the purpose, info about the website, the public key, and yourself.
        - This may follow PKCS #10 specification for formatting
    - Send this to CA and the CA will make a cert with the public key
    - May be a **Registration Authority (RA)** that assists with this process
- **Revoking Certificates**
    - Key compromise
    - CA compromise
    - Change of Affiliation
    - Superseded
    - Cease of Operation
    - Certificate Hold
    - CA creates CRL which tells systems to stop using certain certs.
- **Validating Certs**
    - Systems check if cert is expired, check if the CA issuer is trusted, then query the CA to ensure its valid and not on a CRL.
    - **OCSP - Online Certificate Status Protocol (OCSP)**
        - Allows clients to query the serial number of a cert for status
        - Unknown, good, or revoked.
    - **Key Escrow**
        - Safe environment to hide private key
    - **Recovery Agent**
        - Designated person who can recover or restore keys
        - Typically security professional
        - Sometimes there’s a second private key for emergencies

Exploring Security Policies

- Written security policies are management controls that identify a security plan.
- Security controls and tools should enforce these policies.
- **Personnel Policies**
    - Expectations and Discipline
    - **Acceptable Use Policy**
        - Includes what is or isn't private
        - What users can or cannot do
    - **Mandatory Vacations**
        - At least 5 consecutive business days
        - Prevents embezzlement because the villain should be present to modify files and respond to inquiries
        - Limits the likelihood that one person can cover something up forever
    - **Separation of Duties**
        - Prevents a single person from having complete control over a sector
        - Prevents fraud and mistakes
        - Checks and balances, basically
        - Developers can't implement code with admins testing it
        - IT Admins may have oversight from Security Admins
    - **Job Rotation**
        - Learn processes in each job
        - Increases oversight
        - Prevents collusion
    - **Clean Desk Policy**
        - Ensures protection of secure data
            - No keys, cell phones, access card, sensitive papers, logged-on computers, printouts, passwords, unlocked filing cabinets, or PII
- **Account Management Policies**
    - Least Privilege
    - Account Disablement
    - Admins need Two Accounts
    - No Shared Accounts
- **Third Party Issues**
    - Utilize NDA and Least Privilege
    - Stress
        - Privacy
        - Data Ownership
        - Data Backups
        - Unauthorized Data Sharing
        - Security Policy and Procedures

        - Reviews
- **Interoperability Agreements**
    - **Interconnection Security Agreement (ISA)**
        - Specifies technical and security guidelines for maintaining secure connection and encryption
    - **Service Level Agreement (SLA)**
    - **Memorandum of Understanding (MOU)**
        - Indicates intention to work together for a goal. Less formal than SLA and doesn't include financial penalties.
    - **Business Partner Agreement (BPA)**
        - Details relationship between business partners including obligations, shares, and leaving rules.
- **Change Management Policy**
    - Ensure changes don't cause unintended side-effects
    - Provide accounting and documentation for changes
    - Changes need to be reviewed and approved.
- **Data Policies**
    - **Information Classification**
        - How secure is each bit of data.
        - **Data Labeling and Handling**
            - Not everyone knows how important everything is- unless its labeled.
    - **Data Wiping and Disposal**
        - Get rid of it so its really gone
        - **Bit-level Overwrite**
        - **Degauss the Discks**
        - **Physical Destruction.**
    - **Wiping Files**
        - **Cluster-Tip Wiping**
        - **Bit-Level Wiping**
    - **Storage and Retention Policies**
    - **PII Protection**
    - **Privacy Policy**
        - What info a site can collect and what it can do with that
    - **Social Media Security Usage**
        - **Single-Sign On Risks**
        - **Banner Ads And Malvertisements**
        - **P2P**
            - Can lead to hosting inappropriate data or sharing secure data
- **Responding to Incidents**
    - Incident response team defines different incidents and how to respond
        - Senior Management
        - Network Admin/Engineer

        - Security Expert
        - Communication Expert
    - Team often has extensive training to cope with a variety of situation
    - **Incident Response Procedures**
        - **Preparation**
        - **First Responders**
        - **Incident Identification**
        - **Incident Isolation**
        - **Damage and Loss Control**
        - **Escalation and Notification**
        - **Reporting**
        - **Data Breach**
        - **Recovery/Reconstitution Procedures**
        - **Lessons Learned**
        - **Mitigation Steps**
- Implementing Basic Forensic Procedures
    - **EnCase by Guidance Software**
    - **Forensic Toolkit by AccessData**
    - **Order of Volatility**
        - Order in which to collect evidence before its modified
            - RAM doesn't last, so don't power down a device
        - *Data in cache - processor and hard drive cache*
        - *Data in RAM*
        - *Swap file or paging file*
        - *Data stored on local disks*
        - *Remote logs*
        - *Archived Media*
    - **Capture System Image**
        - Captures the entire contents of a drive
        - Some tools can read data bit-by-bit without modifying it
        - Dd command in Linux
    - Take Hashes
    - Analyze copies, not original
    - Network Traffic and Logs
        - Look for MAC addresses of possible suspects
        - Protocol analyzers can help monitor traffic
        - Trace IP to ISP
    - Chain of Custody
        - Indicate everyone who touched evidence and where it was stored
    - Capture Video CCTV
    - Record Time Offset
        - Time zone changes?
    - Screenshots

    - Witnesses
    - Track Man-Hours and Expense
    - Big Data Analysis
- **Raising Security Awareness**
    - Security Policy Training and Procedures
    - Role-Based Training
        - Executive Personnel
        - Incident Response Team
        - Administrators
        - End Users
    - Can Include
        - Security Policy Contents
        - Keeping Cipher Codes Private
        - Acceptable Use and user responsibilities
        - PII
        - Data labeling, handling, and disposal
        - Information classification
        - Compliance with laws, practices, and standards
        - Threat awareness including malware and phishing
        - User habits that present risks
        - Social Networking and P2P
- **Training and Compliance Issues**
    - **Metrics to Validate Compliance**
        - Measure security incidents

Extra Ports Info!

- Well-known/System Ports
    - 0-1023
- User Ports/Registered Ports
    - 1024-49151
- Dynamic/Private/Ephemeral Ports
    - 49152-65535
- Port Numbers and their Applications
    - 20 - FTP (Send file data)
    - 21 - FTP (Session info)
    - 22 - SSH, SFTP, SCP
    - 23 - Telnet
    - 25 - SMTP
    - 49 - TACACS+
    - 53 UDP/TCP - DNS

- 67 UDP - DHCP and BOOTP
- 69 - TFTP
- 80 - HTTP
- 88 - Kerberos
- 110 - POP3
- 119 - NNTP (Network News Transfer Protocol)
- 123 - NTP (Network Time Protocol)
- 137,138,139 - NetBIOS
- 143 - IMAP
- 161 - SNMP (Agents receive requests)
- 162 - SNMP (Controller receives data)
- 389 - TCP - LDAP Lightweight Directory Access - 389
- 443 - HTTPS (over TLS/SSL)
- 443 - SSTP (Over TLS/SSL) Secure Socket Tunneling Protocol
- 445 - SMB Server Messaging Block - 445
- 465 - SMTP Secure Mail Transfer Protocol
- 500 - IKE Internet Key Exchange
- 636 - LDAPS w/ TLS
- 989/990 - FTPS
- 1701 - L2TP, L2F Layer 2 Tunneling Protocol - 1701
- 1720 - H.323
- 1723 - PPTP Point to Point Transfer Protocol - 1723
- 1812,1813 - RADIUS RADIUS - 1813,1812
- 2427 - MGCP Media Gateway Control Protocol - 2427
- 2727 - MGCP
- 3389 - RDP Remote Desktop Protocol - 3389
- 5004 - RTP Real-time Transport Protocol - 5004
- 5005 - RTP (Default)
- 5060 - SIP (unencrypted) Session Initiation Protocol - 5060
- 5061 - SIP (encrypted with TLS)

- **Protocol IDs**
  - PID 50 - ESP IPsec IPsec
  - PID 51 - AH IPsec Authentication Headers