Complete Course

Security +

CompTIA Security+

AB

Security +

CIA Security:

1. **Confidentiality** = Encryption (Ensure That Only Authorized Users Can Access The Data)
2. **Integrity** = Hashing (Ensure That The Data Is Not Modified Without Permission)
3. **Availability** = Ex: 404 not found (Ensure That The Data Is Available)

AAA Security:

1. **Authentication** = Ex: Username
2. **Authorization** = Ex: Password
3. **Accounting** = Ex: Log Files

Non-Repudiation: Proof That Someone Do Something.

Four Main Threats:

1. **Malware:** Short-hand Term For Malicious Software.(Virus, Warm, ...)
2. **Unauthorized Access:** When Access Computer Resource And Data Without Owner Approve.
3. **System Failure:** Computer Crashes.(Ex: BSOD "Blue Screen Of Death")
4. **Social Engineering:** Manipulating Users. (Ex: Phishing)

Mitigating Threats:

1. **Physical:** Ex: Alarm, Locks, Security Gard, ...
2. **Technical:** Ex: Smart Cards, IDS, Encryption, ...
3. **Administrative (Procedures, Law):** Ex: Policies, DRP, Security Awareness, ...

Five Types Of Hackers:

1. **White Hats:** Non-malicious Hacker. (Ex: Pen Tester)
2. **Black Hats:** Malicious Hacker. (Ex: Bad Guy)
3. **Gray Hats:** Hackers Doesn’t Belong To Company. (Ex: He's Doing It For Fun)
4. **Blue Hats:** Hack With Permission Of The Company But Are Not Employed.
5. **Elite:** Hackers Find And Exploit Vulnerabilities Before Anyone Else.

Threat Actors (From Bottom To Top):

1. **Script Kiddies:** Hackers Who Only Use Tools And Exploit Written By Others. (Ex: Baby Hacker)
2. **Hacktivists:** Hackers Who Are Driven By A Cause Like Social Change. (Ex: Anonymous)
3. **Organized Crime:** Hacker Who Are Part Of A Crime.
4. **Advanced Persistent** Threats (APT): Hacker Supported By Nation States.

Malware:

1. **Virus:** Malicious Code That Runs Without Users Knowledge. (Require User Action)
   a. **Boot Sector:** Virus Stored In The Firs Sector Of Hard Drive.
   b. **Macro:** Virus Embedded Into A Document.
   c. **Program Virus:** Virus Infect An Executable Or Application.
   d. **Multipartite:** Boot Sector + Program Virus.
   e. **Polymorphic:** Advanced Encrypted Virus That Change Itself Every Time It Is Executed.
   f. **Metamorphic:** Virus That Rewrite Itself. (Advanced Polymorphic)
   g. **Armored:** Virus Have A Layer Of Protection.

2. **Worm:** Like A Virus But Is Able To Copy Itself Without User Interaction.

3. **Trojan Horse:** Malicious Code Disguised As A Not Bad Software.
   a. **Remote Access Trojan(RAT):** Provides Remote Control.

Tool ==> JPS Virus Maker, Pro Rat v1.9

4. **Ransomware:** Malware That Block Users Access To Their Computer System Until They Payoff. (Encrypt Your Files)

5. **Spyware:** Malware Secretly Gathers Information About The User.
   - **Adware:** One Of The Types Of Spyware That Uses For Ads.
   - **Grayware:** Is Not Obviously Malicious or Virus But It Can Still Be Annoying And Harmful.

Tool ==> Wolfeye Keylogger 3.3.

6. **Rootkit:** Software Give Administrative Level Control. (Difficult To Detect)
   - **DLL Injection (Dynamic Link Libraries):** Bad Code Inserted Into Running Process On A Windows Machine.
   - **Driver Manipulation:** An Attack On Kernel-Mode.(System Level)
   - **Shim:** Placed Between Two Things To Intercept Calls And Redirect Them.

6. **Spam:** Activity That Misuse Messaging In Email.
   - **Spim:** Like Spam But In Instant Messaging (IM) Instead Of Email Messaging.

Malware Infections:

1. **Threat Vector:** Method Used To Access Machine.
2. **Attack Vector:** Method Used To Access Machine In Order To Infect It With Malware.

- **Water Hole:** It's A Place That We Return To It Every Single Day. Or It's Malware Is Placed On Website That Victims Will Access. (Ex: Facebook)

Common Delivery Methods: Software, Messaging, Media.

Tool==> Phish Insight On Website.

- Botnet & Zombies: Common Used DDoS.

Zombies Is a Part Of Botnet Which Is: A Collection Of Computers That Are Hacked, Control It One Device. (Hacker Send Any Attack Method From Device That Have Control On It)

Active Interception: Occurs When A Computer Is Placed Between Sender And Receiver And Is Able To Capture Or Modify The Traffic.

Privileged Escalation: Occurs When You Are Able To Exploit Error In Design To Gain Access To Resources.

Back Door: Are Used To Bypass Normal Security And Authentication Function.

Easter Egg: These Easter Eggs Are Hidden Surprises Which Are Inserted By Developers. This Kind Of Easter Eggs Are Fun, But Can Also Open Up a Hidden Back Door To Attackers.

Logic Bomb: Malicious Code Inserted Inside A Program Execute Only When Some Conditions Have Been Done.

Removing Malware:

1. Identify Symptoms Of A Malware Infection.
2. 2.Quarantine The Infected Systems. (So Can't Infect Another Computers)
3. Disable System Restore. (If Was Windows)
4. Remediate The Infected System.
5. Schedule Automatic Update And Scans.
6. Enable System Restore And Create A New Restore Point.
7. Provide End User Security Awareness Training.

Security Applications And Devices:

1. Windows Firewall ==> For Windows Os
2. PF and IPFW ==> For Mac Os
3. iptables ==> For Linux Os

Intrusion Detection System (IDS): Device Or Software That Monitors A System Or Network And Analyzes The Data Passing. (Just Alert And Log Activity)

a. Host IDS (HIDS)
b. Network (NIDS)

They Based On:

1. **Signature:** Specific String Of Bytes Triggers An Alert.
2. **Policy:** Relies On Specific Declaration Of The Security Policy.
3. **Anomaly:** Analyzes The Current Traffic And Triggers An Alert if It Was Bad Behavior.

Four Types Of Alert:

1. **True Positive:** Yes Attack, Yes Alert.
2. **True Negative:** No Attack, No Alert.
3. **False Positive:** No Attack, Yes Alert.
4. **False Negative:** Yes Attack, No Alert.

IPS: Same IDS But It Can Prevent Attacks.

Pop-up Blockers: To Block Ads.

Content Filters: Blocking Of External Files Containing JavaScript, Images, Or Web pages From Loading In A Browser.

Best Protection ==> Ensure Your Browser And It's Extensions Are Updated.

Data Loss Prevention (DLP): Monitors The Data Of System While In Use, In Transit, Or At Rest To Detect Attempts To Steal The Data.

1. **Endpoint DLP System:** Software Client That Monitors The Data And Can Stop A File Transfer Or Alert Admin. (Same IDS But Focus On Data)
2. **Network DLP System:** Software Or Hardware That Installed On The Network To Detect Data In Transit.
3. **Storage DLP System:** Software Installed On Servers In The Datacenter Scan The Data At Rest.
4. **Cloud DLP System:** Cloud Software As A Service That Protects Data Being Stored In Cloud Services.

Basic Input Output System (BIOS): Firmware That Provides The Computer Instructions For How To Accept Input And Send-output.

Unified Extensible Firmware Interface (UEFI): Same Basic Input Output System.

To Secure The BIOS:

1. Flash The BIOS: Insure Update For BIOS.
2. Use A BIOS Password.
3. Configure The BIOS Boot Order.
4. Disable The External Ports And Devices.
5. Enable The Secure Boot Option.

Removable Media Controls: Technical Limitations Placed On A Removable Media.(Like: USB)

Network Attached Storage (NAS): Storage Devices That Connect Directly To Your Organization's Network.

Storage Area Network (SAN): Network Designed Specifically To Perform Block Storage Functions That May Consist Of NAS Devices.

If You Use Single NAS There 3 Tips To Ensure That You Are Secure:

1. Use Data Encryption.
2. Use Proper Authentication.
3. Log NAS Access.

Encryption ==> Ensure Confidentiality

Disk Encryption:

1. **Self-Encryption Drive (SED):** Storage Device That Performs Whole Disk Encryption By Using Embedded Hardware.
2. **Software Encryption** (Like: In MAC -FileVault-, In Windows -BitLocker-)
3. **Hardware Security Module (HSM):** Physical Devices That Act As A Secure Cryptoprocessor During The Encryption Process.

Trusted Platform Module (TPM): Chip Residing On The Motherboard That Contains An Encryption Key.

Advanced Encryption Standard (AES): Symmetric Key Encryption That Supports 128-bit And 256-bit Keys.

Mobile Security:

WiFi Protected Access (WPA2): Is The Highest Level Of Wireless Security. ==> Algorithm Is AES -Advanced Encryption Standard-

Protect Mobile Against Malware:

1. Ensure You Have Anti-virus Solution.
2. Ensure Your Mobile Device Is Patched And Updated.
3. Only Install Apps From Official App Store Or Play Store.
4. Don't Jailbreak/root Device.
5. Don’t Use Custom Firmware Or Custom ROM.

Subscriber Identity Module (SIM): Integrated Circuit That Securely Stores The International Mobile Subscriber Identity (IMSI) Number And It's Related Key.

SIM Cloning: Allows Tow Phones To Utilize The Same Service And Allows An Attacker TO gain Access To The Phones Data.

Bluetooth Attack:

1. **Bluejaking:** Sending Of Unsolicited Messages To Bluetooth Enabled Devices. (Sends Information To A Device)
2. **Bluesnarfing:** Unauthorized Access Of Information From A Wireless Device Over A Bluetooth Connection. (Takes Information From A Device)

Remote Lock: Requires A Pin Or Password Before Someone Can Use The Device.

Remote Wipe: Remotely Erases The Contents Of The Device To Ensure The Information Is Not Received By The Thief.

- Mobile Device Management: Software Solution That Allows System Administrators To Create Policies Over Its Mobile Device.

Geotagging: Embedding Of The Geolocation Coordinates Into A Piece Of Data. (Ex: Photo)

HTTPS ==> Transport Layer Secure (TLS)

Bring Your Own Device (BYOD):

- **Storage Segmentation:** Creating Separation Between Personal And Company Data On A Single Device.
- **Mobile Device Management (MDM):** Software Solution For Remote Administration And Configuration Of Mobile Devices. (It Can Prevent Special Apps From Being Installed On The Device)

Choose Your Own Device (CYOD).

To Protect Mobile Device:

1. Update Your Device To The Latest Version.
2. Install Antivirus.
3. Train Users On Proper Security And Use Of The Device.
4. 4.Only Install Apps From The Official Store.
5. Don't Jailbreak/root Your Device.
6. Only Use v2 SIM Cards.
7. Turn Off All Unnecessary Features.
8. Turn On Encryption For Voice And Data.
9. Use Strong Password.
10. Don't Allow BYOD.
11. Good Security Policy.

Hardening: Act Of Configuring An OS Securely By Updating It, Creating Rules And Policies, And Removing Unnecessary Applications And Services. (Minimize The Risk)

Least Functionality: Process Of Configuring Workstation Or Server To Only Provide Essential Applications And Services. (Provide Basic Functions)

System Center Configuration Management (SCCM): Provides Remote Control, Patch Management, Software Distribution, Operating System Deployment, Network Access Protection And Hardware And Software Roster.

Application Whitelist: Only Apps That Are On The List Are Allowed To Be run By The OS While Others Will Blocked. (Unlike Application Blacklist Which Is More Easy To Setup And More Common)

Trusted OS (TOS): An OS That Meets The Requirements Set Forth By Government And Has Multilevel Security.

Patches Or Hotfix: A Single Problem-fixing Piece Of Software For An OS Or Apps.

Five Categories Of Updates:

1. **Security Update:** Software Code That Is Release For A Product-specific Vulnerability.
2. **Critical Update:** Software Code For A Specific Problem Addressing A Critical, Non-Security Bug In The Software.
3. **Service Pack:** Group Of Patches (Hotfixes), Security Updates, Critical Updates, And Possibly Some Feature Or Design Changes.
4. **Windows Update:** Update To Fix A Non Critical Problem, As Well As To Provide Additional Features.
5. **Driver Update:** Updated Device Driver To Fix Security Issue Or Add A Feature To A Supported Piece Of Hardware.

Patch Management: Process Of Planning Testing, Implementing, And Auditing Of Software Patches.

There Is 4 Steps For It:

1. **Planning:** Microsoft Baseline Security Analyzer (MBSA) To Determine Security Misconfiguration.
2. **Testing.**
3. **Implementing.**
4. **Auditing.**

Windows Update Service Called ==> wuauserv

Group Policy: Set Of Rules That Can Be Applied To A Set Of Users Within OS.

Security Template: A Group Of Polices That can Be Loaded Through One Procedure.

Baselining: Process Of Measuring Changes In the Network, Hardware, And Software Environment.

File System➔ NTFS, FAT32, ext4, HFS+, APFS.

- Windows Can Utilize ==> NTFS, FAT32.
- Linux ==> ex4
- OSX ==> APFS

New Technology File System (NTFS): It's The Default File System For Windows And More Secure Because It Supports Logging, Encryption, larger Partition Size, And Larger File Size Than FAT32.

To Convert Form FAT32 To NTFS:

Open The Command Line And Write:

```
convert G: /FS:NTFS
```

Five Things You Have To Do To Easy Recovery From Hard Drives:

1. Remove Temporary Files By Using Disk Cleanup.
2. Periodic System File Checks.
3. Defragment Your Disk Drive.
4. Back UP Your Data.
5. Use And Practice Restoration Techniques.

Virtualization: Creation Of A Virtual Resource.

1. **System Virtual Machine:** Complete Platform Designed To Replace An Entire Physical Computer And Includes A Full Desktop/Server OS.
2. **Processor Virtual Machine**: Designed To Only Run A Single Process Or Application Like A Virtualized Web Browser Or Simple Web Server.

Hypervisor: Manages the Distribution Of The Physical Resources Of A Host Machine (Server) To The Virtual machines Being Run (Guests).

Threat Of VM: Vm's Are Separated.

1. **VM Escape:** An Attack That Allows Attacker To Break Out Of A Normally Isolated VM By Interacting Directly With The Hypervisor.
2. **Elasticity:** It's The Ability To Scali Up Or Scali Down.
3. **Data Remnants:** Contents Of A VM That Exist As Deleted Files On A Cloud-based Server After Deprovisioning Of A VM.
4. **Privilege Elevation:** Occurs When A User Is Able To Grant Themselves the Ability To Run Functions As A Higher-level User.
5. **Live Migration:** Occurs When A VM is moved From One Physical Server To Another Over The Network.
6. **Virtualization Sprawl:** Occurs When VM's Are Created, Used, And Deployed Without Proper Management Or Control By The System Admins.

Application Security:

General Security For Web Browsers:

1. Implement Policies.
2. Train Your Users.
3. Use Proxy (Reduce Requests And Bandwidth) & Content Filter (Blacklist).
4. Prevent Malicious Code.

Cookies: Text Files Placed On A Client's Computer To Store Information About The Users Browsing Habits, Credentials, And Other Data.

- **Tracking Cookies:** Used By Spyware.
- **Session Cookies:** Used To Maintain The Connection Between You And The Server.

Locally Shared Object (LSO -Flash Cookies-): They Are Stored In Your Windows User Profile Under The Flash Folder Inside Of Your AppData Folder.

Add-Ons: Smaller Browser Extension And Plugins That Provide Additional Functionality To The Browser.

Advanced Security Options: Browser Configuration And Settings For Numerous Options Such As SSL/TLS Settings, Local Storage/Cache Size, Browsing History, And Much More.

User Account Control: Prevents Unauthorized Access And Avoids User Error In The Form Of Accidental Changes.

Software Development Life Sycle (SDLC): Is An Organized Process Of Developing A Secure Application.

1. Planning And Analysis.
2. Software/System Design.
3. Implementation.
4. Testing.
5. Integration.
6. Deployment.
7. Maintenance.

- **DevOps:** Software Development And information Operations.
- **Least Privilege:** Users And Processes Should Be Run Using The Least Amount Of Access.
- **Defense In Depth:** Layering Of Security Controls.
- **Never Trust User Input:** Any Input Is Received From A User Should Undergo Input Validation Prior To Allowing It To Be Utilized By An Application.
- **Minimize Attack Surface:** Reduce The Amount Of Code Used By A Program, Eliminate Unneeded Functionality, And Require Authentication Prior To Running Additional Plugins.
- **Create Secure Defaults:** Default Installations Should Include Secure Configurations Instead Of Requiring An Administrator Or user To Add in Additional Security.
- **Authenticity And Integrity:** Apps Should Be Deployed Using Code Signing To Ensure The Program Is not Changed Inadvertently Or Maliciously Prior To Delivery To An End User.
- **Fail Securely:** Apps Should Be Coded to properly Conduct Error handling For Exceptions In Order To fail Securely Instead Of Crashing.
- **Fix Security Issues:** If A Vulnerability Is Identified, Then It Should Be Quickly And Correctly Patched To Remove The Vulnerability.
- **Rely On Trusted SDKs (Software Development Code):** SDKs Must Come From Trusted Sources To Ensure No Malicious Code Is Being Added.

System Testing:

1. **Black-Box Testing:** Occurs When A Tester Is Not Provided With Any Information About The System Or Program Prior To Conducting The Test.
2. **White-Box Testing:** Occurs When A Tester Is Provided Full Details Of The System Including The Source Code, Diagrams, And User Credentials In Order To Conduct The Test.
3. **Gray-Box Testing:** Mix From White And Black Ex: Given User Credentials But Not Admin Credentials.

Structured Exception Handling (SEH): Provides Control Over What The App Should Do When Faced With A Runtime Or Syntax Error.

Input Validation: Applications Verify That Information Received From A User Matches A Specific Format Or Range Of Values.

Static Analysis: Source Code Of An Application Is Reviewed Manually Or With Automatic Tools Without Running The Code.

Dynamic Analysis: Analysis And Testing Of A Program Occurs While It Is Being Executed Or Run.

Fuzzing: Injection Of Randomized Data Into A Software Program In An Attempt To Find System-Failures, Memory leaks, Error Handling Issues, And Improper Input Validation.

Types Of Exploit Of Development:

1. **Backdoors:** Code Placed In Computer Programs To Bypass Normal Authentication And Other Security Mechanisms. (Poor Coding Practice)
2. **Directory Traversal:** Method Of Accessing Unauthorized Directories By Moving Through The Directory Structure On A Remote Server.
3. **Arbitrary Code Execution:** Occurs When An Attacker Is Able to Execute Or Run Commands On A Victim Computer.
4. **Remote Code Execution (RCE):** Occurs When An Attacker Is Able to Execute Or Run Commands On Remote Computer.
5. **Zero Day:** Attacks Against A Vulnerabilities that Is Unknown To The original Developer Or Manufacturer.
6. **Buffer Overflow:** Occurs When A Process Stores Data Outside The Memory Range Allocated By The Developer.
    a. **Buffer:** A Temporary Storage Area That A Program Uses To Store Data.
    b. **Stack:** Reserved Area Of Memory Where The Program Saves The Return Address When A Function Call Instruction Is Received.
    c. **Smash The Stack:** Occurs When An Attacker Fills Up The Buffer With NOP (None Operation Instructions) So that The Return Address May Hit A NOP And Continue On Until It Finds the Attackers Code To Run.
    d. **Address Space Layout Randomization (ASLR):** Method Used By Programmers To Randomly Arrange The Different Address Spaces Used By A Program Or Process to Prevent Buffer Overflow Exploits.
7. **Cross-Site Scripting (XSS):** Occurs When An Attacker Embeds Malicious Scripting Commands On A Trusted Website.
    a. **Stored/Persistent:** Attempts To Get Data Provided By The Attacker To Be Saved On The Web Server By The Victim.
    b. **Reflected:** Attempts To Have A Non-Persistent Effect Activated By A Victim Clicking A Link On The Site.
    c. **DOM-based:** Attempts To Exploit The Victims Web Browser.
8. **Cross-Site Request Forgery (XSRG/CSRF):** Occurs When An Attacker Forces A User To Execute Actions on a Web Server For Which they Are Already Authenticated.

To Prevent It: Encryption, XML Scanning, Cookie Verification.

9. **SQL Injection (Structured Query Language):** Attack Consisting Of The Insertion Or Injection Of An SQL Query Via Input Data From The Client to A Web Application.
   Injection Attack: Insertion Of Additional Information Or Code Through Data input From A Client To An Application.

Network Security:

OSI Model: Used To Explain Network Communications Between A Host And Remote Device Over A LAN Or WAN.

1. **Physical Layer:** Represents The Actual Network Cables And Radio Waves Used To CArry Data Over A Network (Bits).
2. **Data Link Layer:** Describes How A Connection Is Established, Maintained, And Transferred Over The Physical Layer And Uses Physical Addressing (MAC Address).
3. **Network Layer:** Uses Logical Address (IP Address) To Router Or Switch Information Between Hosts, The Network, And The Internetworks (Packet).
4. **Transport Layer:** Manages And Ensures Transmission Of The Packets Occurs From A Host To A Destination Using Either TCP (Segments) Or UDP (Datagrams).
5. **Session Layer:** Manages The Establishment, Termination, And Synchronization Of A Session Over The Network.
6. **Presentation Layer:** Translates The Information Into A Format That The Sender And Receiver Both Understand.
7. **Application Layer:** Layer From Which The Message Is Created, Formed, And Originated. (Ex: HTTP, SMTP, FTP)

Switches (Layer 2 MAC Address): Are The Combined Of Hubs And Bridges. (Reduce Traffic And Increase Security)

- **MAC Flooding:** Attempt To Flood The Limited Switch Memory Set Aside To Store The MAC Addresses For Each Port.
- **MAC Spoofing:** Occurs When An Attacker Makes Their Own MAC address To Pretend They have The MAC Address Of Another Device.
- **Physical Tempering:** Occurs When An Attacker Attempts To Gain Physical Access.

Routers (Layer 3 IP Address): Used To connect Two Or More Networks To Form An Internetwork.

- **Access Control List (ACL):** An Ordered Set Of Rules That A Router Uses To Decide Whether To Permit Or Deny Traffic Based Upon Given Characteristics. (IP Spoofing Is Used To Trick A Routers ACL)

Three Types Of Network Zones:

1. **LAN.**
2. **WAN.**
3. **De-Militarized Zone (DMZ):** Focused On Providing Controlled Access to Publicly Available Servers That Are Hosted Within Your Organizational Network.

- **Extranet:** Specialized Type Of DMZ That Is Created For your Partner Organizations To Access Over A Wide Area Network.
- **Network Access Control (NAC):** Security Technique In Which Devices Are Scanned To Determine Its Current State Prior To Being Allowed Access Onto A Given Network.

Persistent Agents: A Piece of Software That Is Installed On The Device Requesting access To The Network.

Non-Persistent Agents: Uses A Piece Of Software That Scans The Device Remotely Or Is Installed And Subsequently Removed After The Scan.

- **Switch Spoofing:** Attacker Configures Their Device To Pretend It Is A Switch And Uses It To Negotiate A Trunk Link To Break Out Of A VLAN.
- **Double Tagging:** Attacker Adds An additional VLAN Tag To Create An Outer And Inner Tag.

- **Subnetting:** Act Of Creating Subnetworks logically Through the Manipulation OF IP Addresses.

- **Network Address Translation (NAT):** Process of Changing An IP Address while It Transits Across A Router.
- **Prot Address Transation (PAT):** Router Keeps Track Of Requests From Internal Hosts By Number Ports For Each Request.
  - Class A: 10.0.0.0 - 10.255.255.255
  - Class B: 172.16.0.0 - 172.31.0.0
  - Class C: 192.168.0.0-192.168.255.255

Telephony: Term Used To Describe Devices That Provide Voice Communication To Users.

Modem: A Device That Could Modulate Digital Information Into An Analog Signal For Transmission Over A Standard Dial-Up Phone Line.

Public Branch Exchange (PBX): Internal Phone System Used In Large Organizations.

Voice Over Internet Protocol (VOIP): Digital Phone Service Provided By Software Or Hardware Devices Over A Data Network.

Perimeter Security:

Perimeter Security: Security Devices Focused On The Boundary Between The LAN And The WAN In Your Organization's Network.

Firewalls: Screen Traffic Between Two Portions Of A Network. (Protect Network From Another)

Firewalls Types: Hardware, Software, Embedded.

Packet Filtering: Inspects Each Packet Passing Through The Firewall And Accepts Or Rejects It Based On The Rules.

Inpund ==> Port 80 (Web Traffic), Prot 443 (Secure Web Traffic).

Packet Filtering Types:

1. **Stateless:** Accepts Or Rejects It Based On IP Address And Port Number.
2. **Stateful:** Tracks The Request Leaving The Network.

NAT Filtering: Filters Traffic Based On The Ports Being Utilized And Type Of Connection (TCP / UDP).

Application Layer Gateway (ALG): Conducts An In-Depth Inspection Based On The Application Being Used (FTP, Telnet).

Circuit-level Gateway: Operates At The Session Layer And Only Inspects the Traffic During The Establishment Of The initial Session Over TCP or UDP.

MAC Filtering: Refers To A Security Access Control Method The MAC Address Assigned To Each Network.

- **Explicit Allow:** Traffic Is Allowed To Enter Or Leave The Network Because There Is An ACL rule That Specifically Allows It.
- **Explicit Deny:** Traffic Is Denied The Ability To Enter Or Leave The Network Because There Is An ACL rule That Specifically Allows It.
- **Implicit Deny:** Traffic Is Denied The Ability To Enter Or leave The Network Because There Is No Specific Rule That Allows It.

Most Operate Layer3 (Blocking IP Addresses) And Layer4 (Blocking Ports).

Web Application Firewall (WAF): Firewall Installed To Protect Your Server By Inspecting Traffic Being Sent To A Web Application. (Can Prevent XSS Or SQL Injection)

Proxy Server: A Device That Acts As A Middle man Between A Device And Remote Server.

Proxy Types:

1. **IP Proxy:** Is Used To Secure A Network By Keeping Its Machines Anonymous During Web Browsing.
2. **Caching Proxy:** Attempts To Server Client Requests By Delivering Content From Itself Without Actually Contacting The Remote Server.
3. **Content Filter:** Used In Organizations To Prevent Users From Accessing Prohibited Websites And Other Content.
4. **Web Security Gateway:** A Go-Between Device That Scans For Viruses, Filters Unwanted Content, And Performs Data Loss Prevention Functions.

Honeypots And Honeynets: Used to Attract And Trap Potential Attackers.

Honeypots: Single Computer (Or File, Files, or IP Range) That Might Be Attractive To An Attacker.

Honeynets: A Group Of Computers, Servers, Or Networks Used To Attract An Attacker.

Data Loss Prevention (DLP): Systems Designed To Protect Data By Conducting Content Inspection Of Data Being Sent Out Of The Network, Also Called Information Leak Protection (ILP) Or Extrusion Prevention Systems (EPS), It Is Used To Ensure Private Data Stay Secure.

Network Intrusion Detection Systems (NIDS): Attempts To Detect, Log, And Alert On Malicious Network Activities, It Is Use Promiscuous Mode To See All Network Traffic On A Segment.

Network Intrusion Prevention Systems (NIPS): Attempts To Remove, Detain, Or Redirect Malicious Traffic, It Is Installed In-Line Of The Network Traffic Flow. , It can Be Also Perform Functions As A Protocol Analyzer.

Unified Threat Management (UTM): Combination Of Network Security And Technologies To Provide More Defense In Depth Within A Single Device, It Is Also Known As A Next Generation Firewall (NGFW).

Cloud Computing: A Way Of Offering On-Demand Services That Extend The Traditional Capabilities Of A Computer Or Network.

Hyperconvergence: Allows Providers To Fully Integrate The Storage, Network, And Servers.

Virtual Desktop Infrastructure (VDI): Allows A Cloud Provider To Offer A Full Desktop OS To An End User From A Centralized Server.

Cloud Types:

1. **Public:** A Service Provider Makes Resources Available To The End Users Over The Internet. (Google Drive)
2. **Private:** A Company Creates Its Own Cloud Environment That Only Can Utilize As An Internal Enterprise Resource.
3. **Hybrid:** Public + Private.
4. **Community Cloud:** Resources And Costs Are Shared Among Several Different Organizations Who Have Common Service Needs.

As A Service:

1. **Software As A Service (SaaS):** Provides All The Hardware, OS, Software, And Applications Needed For A Complete Service To Be Delivered.
2. **Infrastructure As A Service (IaaS):** Provides The Hardware, OS, Software, And Backend Software Needed In Order To Develop Your Own Software Or Service.
3. **Platform As A Service (PaaS):** Provides Your Organization With The Hardware And Software Needed For A Specific Service To Operate.
4. **Security As A Service (SECaaS):** Provides Your Organization With various Types Of Security Services Without The Need To Maintain A Cybersecurity Staff.

Sandboxing: Utilizes Separate Virtual Networks To Allow Security Professionals To Test Suspicious Or Malicious Files.

File Servers: Servers Are Used To Store, Transfer, Migrate, Synchronize, And Archive Files For Your Organization.

FTP Server: A Specialized Type Of File Server That Is Used To Host Files For Distribution Across The Web.

Domain Controller: A Server That Acts As A Central Repository Of All The User Accounts And Their associated Passwords For The Network.

Network Attacks:

Port: A Logical Communication Endpoint That Exists On A Computer Or Server.

Inbound Port: A Logical Communication Opening On A Server That Is Listening For A Connection From A Client.

Outbound Port: A Logical Communication Opening Created On A Client In Order To Call Out To Server That Is Listening For A Connection.

- **Ports: 0-65,535**

1. **Well Known Ports:** Prots 0 To 1023 Are Considered Well-known And Are Assigned By The Internet Assigned Numbers Authority (IANA).
2. **Registered Ports:** Ports 1024 To 491515 Are Considered Registered And Are Usually Assigned To Proprietary Protocols.
3. **Dynamic Or Private Ports:** Ports 49152 To 65535 Can Be Used By Any Application Without Being Registered With IANA.

21 TCP= FTP: File Transfer Protocol Is Used To Transfer Files From Host To Host.

22 TCP/UDP= SSH, SCP, SFTP: Secure Shell Is Used To Remotely Administer Network Devices And Systems. SCP Is Used For Secure Copy And SFTP For Secure FTP.

23 TCP/UDP= Telnet: Unencrypted Method To Remotely Administer Network Devices (Should Not Be Used).

25 TCP= SMTP: Simple Mail Transfer Protocol Is Used To Send Email Over The Internet.

53 TCP/UDP= DNS: Domain Name Service Is Used To Resolve Hostnames To IPs And IPs To Hostnames.

69 UDP= TFTP: Trivial FTP Is Used As A Simplified Version Of FTP To Put A File On A Remote Host, Or Get A File From A Remote Host.

80 TCP= HTTP: Hyper Text Transfer Protocol Is Used To Transmit Web Page Data To A Client For Unsecured Web Browsing.

88 TCP/UDP= Kerberos: Used For Network Authentication Using A System Of Tickets Within A Windows Domain.

110 TCP= POP3: Post Office Protocol v3 Is Used To Receive Email From a Mail Server.

119 TCP= NNTP: Network News Transfer Protocol Is Used To Transport Usenet Articles.

135 TCP/UDP= RPC/DCOM-scm: Remote Procedure Call Is Used To Locate DOCM Ports To Request A Service From A Program On Another Computer On The Network.

137-139 TCP/UDP= NetBIOS: Is Used To Conduct Name Querying, Sending Of Data, And Other Functions Over A NetBIOS Connection.

143 TCP= IMAP: Internet Message Access Protocol Is Used To Receive Email From A Mail Server With More Features Than POP3.

161 UDP= SNMP: Simple Network Management Protocol Is Used To Remotely Monitor Network Devices.

162 TCP/UDP= SNMPTRAP: Used To Send Trap And Inform Requests To The SNMP Manager On A Network.

389 TCP/UDP= LDAP: Lightweight Directory Access Protocol Is Used To Maintain Directories Of Users And Orther Objects.

443 TCP= HTTPS: Hyper Text Transfer Protocol Secure Is Used To Transmit Web Pages Data To A Clinet Over An SSL/TLS Encrypted Connection.

445 TCP= SMB: Server Message Block Is Used To Provide Shared Access To Files And Other Resources On A Network.

465/587 TCP= SMTP with SSL/TLS: Simple Mail Transfer Protocol Is Used To Send Email Over The Internet With An SSL And TLS Secured Connection.

514 UDP= Syslog: Is Used To Conduct Computer Message Logging, Especially For Routers And Firewall Logs.

636 TCP/UDP= LDAP SSL/TLS: Used To Maintain Directories Of Users And Other Objects Over An SSL/TLS Encrypted Connection.

860 TCP= iSCOSI: Is Used For Linking Data Storage Facilities Over IP.

989/990 TCP= FTPS: File Transfer Protocol Secure Is Used To Transfer Files From Host To Host Over An Encrypted Connection.

993 TCP= IMAP4 With SSL/TLS: Internet Message Access Protocol Is Used To Receive Email From A Mail Server Over An SSL/TLS Encrypted Connection.

995 TCP= POP3 With SSL/TLS: Post Office Protocol v3 Is Used To Receive Email From a Mail Server Over An SSL/TLS Encrypted Connection.

1433 TCP= MS-sql-s: Microsoft SQL Server Is Used To Receive SQL Database Queries From Client.

1645/1646 UDP= RADIUS (alternative): Remote Authentication Dial-In User Service Is Used For Authentication And Authorization (1645) And Accounting (1646).

1701 UDP= L2TP: Layer 2 Tunnel Protocol Is Used As An Underlying VPN Protocol But Has No Inherent Security.

1723 TCP/UDP= PPTP: Point-to-Point Tunneling Protocol Is An Underlying VPN Protocol With Built-in Security.

1812/1813 UDP= RADIUS: Remote Authentication Dial-In User Service Is Used For Authentication And Authorization (1812) And Accounting (1813).

3225 TCP/UDP= FCIP: Fiber Channel IP Is Used To Encapsulate Fiber Channel Frames Within TCP/IP Packets.

3260 TCP= iSCSI Target: Is A Listening Port For A iSCSI Targeted Devices When Linking Data Storage Facilities Over IP.

3389 TCP/UDP= RDP: Remote Desktop Protocol Is Used To Remotely view And Control other Windows Systems Via A Graphical User Interface.

3868 TCP= Diameter: A More Advanced AAA Protocol That Is A Replacement For RADIUS.

6514 TCP= Syslog Over TLS: It Is Used To Conduct Computer Message Logging, Especially For Routers And Firewalls Logs, Over TLS Encrypted Connection.

Unnecessary Ports: Any Port That Is Associated With A Service Or Function that Is NON-essential to The Operation Of Your Computer Or Network.

DOS: It's Used To Describe Many Different Types Of Attacks Which Attempt To Make A Computer Or Server's Resources Unavailable.

Types:

1. **Flood Attacks:** Attempts To Send More Packets To A Single Server Or Host Than They Can Handle.
   a. **Ping Flood:** An Attacker Attempts To Flood The Server By Sending Too Many ICMP Echo Request Packets (Which Are Known As Pings).
   b. **Smurf Attack:** Attacker Sends A Ping To Subnet Broadcast Address And Devices Reply To Spoofed IP (Victim Server) Using Up Bandwidth And Processing Power.
   c. **Fraggle Attack:** Attacker Sends A UDP Echo Packet To Port 7 (ECHO) And Port 19 (CHARGEN) To Flood A Server With UDP Packets.
   d. **SYN Flood:** Attacker Initiates Multiple TCP Sessions But Never Completes The 3-Way Handshake.
   e. **XMAS Attack:** Network Scan Sets The FIN, PSH, And URG Flags And Can Cause A device To Crash Or Reboot.
2. **Ping Of Death:** An Attack That Sends An Oversized And Malformed Packet To Another Computer Or Server.
3. **Teardrop Attack:** Attack That Breaks Apart Packets Into IP Fragments, Modifies them With Overlapping And Oversized Payloads, And Sends Them To A Victim machine.
4. **Permanent DOS (PDOS):** Attack Which Exploits A Security Flaw To Permanently Break A Networking Device By Reflashing Its Firmware.
5. **Fork Bomb:** Attack That Creates A Large Number Of Processes To Use Up The Available Processing Power Of A Computer.

DDOS: A Group Of Compromised Systems Attack A Single Target Simultaneously To Create A DOS.

DNS Amplification: Attack Which Relies On The Large Amount Of DNS Information That Is Sent In Response To A Spoofed Query On Behalf Of The Victimized Server.

Blackholing Or Sinkholing: Identifies Any Attacking IP Addresses And Routes All Their Traffic To A Non-existent Server Through The Null Interface.

Spoofing: Occurs When An Attacker Masquerades As Another Person By Falsifying Their Identity.

Hijacking: Exploitation Of A Computer Session In An Attempt To Gain Unauthorized Access To Data, Services, Or Other Resources On A Computer Or Server.

Types:

1. **Session Theft:** Attacker Guesses the Session ID For A Web Session, Enabling The To Takeover The Already Authorized Session Of The Client.
2. **TCP/IP Hijacking:** Occurs When An Attacker Takes Over TCP Session Between Two Computers Without The Need Of A Cookie Or Other Host Access.
3. **Blind Hijacking:** Occurs When An Attacker Blindly Injects Data Into The Communication Stream Without Being Able To See If It Is Successful Or Not.
4. **Clickjacking:** Attack That Uses Multiple Transparent layers To Trick A user Into Clicking On A Button Or Link On A Page When They Were Intending To Click On The Actual Page.

5. **Man-in-the-Middle:** Attack That Causes Data To Flow Through The Attackers Computer Where They Can Intercept Or Manipulate The Data.
6. **Man-in-the-Browser:** Occurs when a Trojan infects A Vulnerable Web Browser And Modifies The Web Pages Or Transactions Being Done Within The Browser.
7. **Watering Hole:** Occurs When Malware Is Placed On A Website That The Attacker Knows is Potential Victims Will Access.

Replay Attack: Network-based Attack Where A Valid Data Transmission Is Fraudulently Or Malicious Rebroadcast, Repeated, Or Delayed.

Null Connection: A Connection To The Windows Interposes Communications Share (IPC$).

Transitive Attacks: EX: A=B=C That Means That A=C, In Other Language If Network A Trust In Network B And Network B Trust In Network C That Means That Network A Trust In Network C.

DNS Attack:

1. **DNS Poisoning:** Occurs When The name Resolution Information Is Modified In The DNS Servers Cache.
2. **Unauthorized Zone Transfers:** Occurs When An Attacker Requests Replication Of The DNS Information To Their Systems For Use In Planning Future Attacks.
3. **Alter Hosts Files:** Occurs When An Attacker Modifies The Host File To have The Client Bypass The DNS Server And Redirects Them To An Incorrect Or Malicious Website.
4. **Pharming:** Occurs When An Attacker Redirects one Website That Is Bogus Or Malicious.
5. **Domain Name Kiting:** Attack That Exploits A Process In The Way A Domain name Is Registered So Tat The Domain Name Is Kept In Limbo And Cannot Be Registered By An Authenticated Buyer.

ARP: Protocol For Mapping An Internet Protocol Address (IP Address) To A Physical Machine Address That Is Recognized In The Local Network.

ARP Poisoning: Attack That Exploits The IP Address To MAC Resolution In A Network To Steal, Modify, Or Redirect Frames Within The Local Area Network.

Securing Network:

Default Accounts: A Admin Account That Is Installed On A Device By The Manufacturer During Production.

Weak Password: A Password Should Be Log, Strong, And Complex. This Should Require At Least 14 Characters With A Mix Of Uppercase, Lowercase, Numbers, And Special Characters.

Privilege Escalation: Occurs When A User Is Able To Gain The Rights Of Another User Or Admin.

1. **Horizontal Privilege Escalation:** An Attacker Expands Their Privileges By Taking Over Another Account And Misusing The Valid Privileges Given To The Other User.

2. **Vertical Privilege Escalation:** An Attacker Attempts To Gain More Permissions. Ex: An Attacker Attacks User Account On a Network And Attempts To Gain Administrative Permissions.

Backdoor: A Way Of Bypassing Normal Authentication In A System.

Telnet It Is Not Secure, Use SSH Because It Is Encrypted.

Network Media: Copper, Fiber Optic, And Coaxial Cabling Used As The Connectivity Method In A Wired Network.

UTP Cables Is Commonly Used More Often Than STP.

Electromagnetic Interference (EMI): A Disturbance That Can Affect Electrical Circuits, Devices, And Cables Due To Radiation Or Electromagnetic Conduction, To Minimize That Risk You Should Shielding The Cables.

Radio Frequency Interference (RFI): A Disturbance That Can Affect Electrical Circuits, Devices, And Cables Due The AM/FM Transmission Or Cell Towers, To Minimize That Risk You Should Shielding The Building.

Crosstalk: Occurs When A Signal Transmitted On One Copper Wire Creates An Undesired Effect On Another Wire.

Data Emanation: The Electromagnetic Field Generated By A Network Cable Or Device When Transmitting.

Protected Distribution System (PDS): Secured System Of Cable Management To Ensure That The Wired Network Remains Free From Eavesdropping, Tapping, Data Emanations, And Other Threats.

Service Set Identifier (SSID): Uniquely Identifies The Network And Is The Name Of The WAP Used By The Clients.

Rogue Access Point: An Unauthorized WAP Or Wireless Router That Allows Access To The Secure Network.

Evil Twin: A Rogue, Counterfeit, And Unauthorized WAP With The Same SSID As Your Valid One.

Pre-Shared Key: Same Encryption Key Is Used By The Access Point And The Client.

Three Types Used For Encryption Wireless Network:

1. **Wired Equivalent Privacy (WEP):** Original 802.11 Wireless Security Standard That Claims To Be As Secure As A Wired Network. (Weakness 24-bit IV)
2. **WiFi Protected Access (WPA):** Replacement For WEP Which Uses TKIP, Message Integrity Check (MIC), And RC4 Encryption.
3. **WiFi Protected Access Version 2(WPA2):** 802.11 i Standard To Provide Better Wireless Security Featuring AES With A 128-Bit Key, CCMP, And Integrity Checking.

Briefly:

1. **WEP** ==> IV.
2. **WPA** ==> TKIP And RC4.
3. **WPA2** ==> CCMP And AES.
4. **Open** ==> No Security.

WiFi Protected Setup (WPS): Automated Encryption Setup For Wireless Network At A Push Of A Button, But Is Severely Flawed And Vulnerable.

Jamming: Intentional Radio Frequency Interference Targeting Your Wireless Network To Cause A DOS Condition.

AP Isolation: Creates Network Segment For Each Client When It Connects To Prevent Them From Communicating With Other Clients On The Network.

War Driving: Act Of Searching For Wireless Networks By Driving Around Until You Find Them.

War Chalking: Act Of Physically Drawing Symbols In Public Places To Denote The Open, Closed, And Protected Networks In Range.

IV Attack: Occurs When An Attacker Observes The Operation Of A Cipher Being Used With Several Different Keys And Finds A Mathematical Relationship Between Those Keys To Determine The Clear Text Data.

WiFi Disassociation Attack: Attack That Targets An Individual Client Connected To A Network, Forces It Offline By Deauthenticating It, And Then Captures The Handshake When It Reconnects.

Brute Force Attack: Occurs When An Attacker Continually Guesses A Password Until The Correct One Is Found.

1. **Bluejaking:** Sending Of Unsolicited Messages To Bluetooth Enabled Devices. (Sends Information To A Device)
2. **Bluesnarfing:** Unauthorized Access Of Information From A Wireless Device Over A Bluetooth Connection. (Takes Information From A Device)

Radio Frequency Identification (RFID): Devices That Use A Radio Frequency Signal To Transmit Identifying Information About The Device Or Token Holder. (10 cm to 200 meters)

Near Field Communication (NFC): Allows Tow Devices To Transmit Information When They Are Within Close Range Through Automated Pairing And Transmission. (4 cm)

Physical Security:

1. Surveillance

Closed Circuit TV (CCTV): Wired, Wireless, Pan Tilt Zoom (PTZ).

2. Door Locked: Can use Keys, Pins, Wireless Signals, Or Biometrics.

Mantrap: Area Between Tow Doorways That Holds People Until They Are Identified And Authenticated.

Biometrics: Relies On The Physical Characteristics Of A Person To Identify Them.

False Acceptance Rate (FAR): Rate That A System <u>Authenticates</u> A User As Authorized Or Valid When They Should Not Have Been Granted Access To The System.

False Rejection Rate (FRR): Rate That A System <u>Denies</u> A User As Authorized Or Valid When They Should Have Been Granted Access To The System.

Crossover Error Rate (CER): An Equal Rate (ERR) Where The False Acceptance Rate And False Rejection Rate Are Equal.

Facilities Security:

1. **<u>Fire Suppression</u>:** Process Of Controlling And/or Extinguishing Fires To Protect An Organizations Employees, Data, Equipment, And Buildings.
   a. **Handheld:**
      - Class A ➔ Combustibles Materials.
      - Class B ➔ Flammable Liquids And Gasses.
      - Class C ➔ Electrical Equipment.
      - Class D ➔ Combustible Materials.
      - Class K ➔ Cooking Media.

   b. **Sprinklers:**
      - **Wet Pipe Sprinklers System:** Pipes Are Filled With Water All The Way To The Sprinkler Head And Are Just Waiting For The Bulb To Be Melted Or Broken.
      - **Dry Pipe Sprinklers System:** Pipes Are Filled With Pressurized Air Inly Push Water Into The Pipes When Needed To Combat The Fire.
      - **Pre-Action Sprinkler System:** Will Activate When Heat Or Smoke Is Detected.

   c. **Special Hazard Protection:**
      - **Clean Agent System:** Fire Suppression System That Relies Upon Gas (HALON, FM-200, or CO2) Instead Of Water To Extinguish a Fire.
2. **Heating, Ventilation, And Air Conditioning (HVAC).**
3. **Shielding:**
   a. **Shielded Twisted Pair (STP):** Adds A Layer Of Shielding Inside The Cable.
   b. **Faraday Cage:** Shielding Installed Around An Entire Room That Prevents Electromagnetic Energy And Radio Frequencies From Entering Or Leaving The Room.
   c. **TEMPEST:** U.S. Government Standards For The Level Of Shielding Required In A Building To Ensure Emissions And Interference Cannot Enter Or Exit The Facility.
4. **Vehicles:**
   a. **Controller Area Network (CAN):** Connects All Of A Cars Systems Together In Order For Them To Communicate Effectively.
   b. **Air Gap:** A Method Of Isolating An Entity To Effectively Separate It From Everything Else.

Authentication:

Multi-Factor Authentication: Use of two or more authentication factors to prove a user's identity.

1. **Knowledge:** Password (Word).
2. **Ownership:** Token or smart cards.
3. **Characteristics:** Biometric (finger).
4. **Location:** Where person is trying to login.
5. **Action:** signature.

Time-Based One Time Password (TOTP): A password is computed from a shared secret and current time.

HMAC-Based One Time Password (HOTP): A password is computed from a shared secret and synchronized between the client and the server.

Authentication Models:

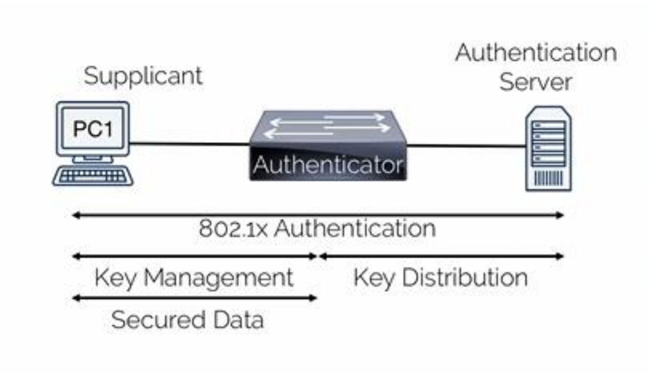
1. **Context-aware Authentication:** Process to check the users or systems attributes or characteristics prior to allowing it to connect.
2. **Single Sign-On (SSO):** A default user profile for each user is created and linked with all of the resources needed.
3. **Federated Identity Management (FIdM):** A single identity is created for a user and shared with all of the organizations in a federation.
    a. **Cross-Certification:** Utilizes a web of trust between organizations where each one certifies others in the federation.
    b. **Trusted Third-Party:** Organizations are able to place their trust in a single third-party (also called the bridge model).

Security Assertion Markup Language (SAML): Attestation model built upon XML used to share federated identity management information between systems.

OpenID: An open standard and decentralized protocol that is used to authenticate users in a federated identity management system.

- OpenID is easier, but SAML is more efficient.

802.1x: Standardized framework used for port-based authentication on wired and wireless network.



- 802.1x can prevent rogue devices.

Extensible authentication Protocol (EAP): A framework of protocols that allows for numerous methods of authentication including passwords, digital certificates, and public key infrastructure.

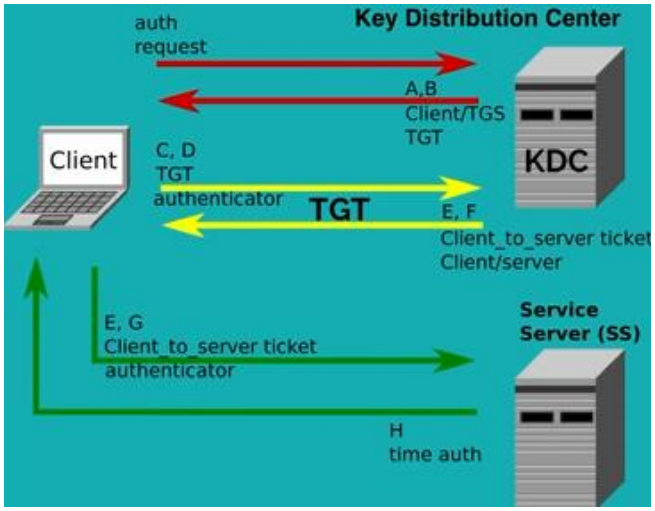
- **EAP-MD5** uses Simple password for its challenge-authentication.
- **EAP-TLS** uses digital certificates for mutual authentication.
- **EAP-TTLS** uses a server-side digital certificate and a client-side password for mutual authentication.

- **EAP-FAST:** Provides flexible authentication via secure tunneling (FAST) by using a protected access credential instead of a certificate for mutual authentication.
- **Protected EAP (PEAP):** Supports mutual authentication by using server certificates and Microsoft's Active Directory to authenticate a client's password.
    - **LEAP** is proprietary to Cisco-based networks.

<u>**Lightweight Directory Access Protocol**</u> **(LDAP):** A database used to centralize information about clients and objects on the network. (Like **Active Directory** for <u>Microsoft version</u>)

- For Unencrypted **Port 389.**
- For Encrypted **Port 636.**

Kerberos: An authentication protocol used by windows to provide for two-way (mutual) authentication using a system of tickets. **Use Port 88**

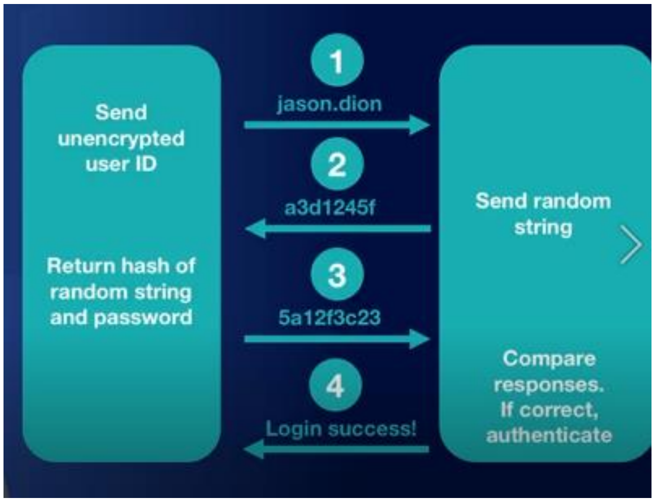


Remote Desktop Protocol (RDP): Microsoft's proprietary protocol that allows administrators and users to remotely connect to another computer via a GUI. **Use Port 3389**

Virtual Network Computing (VNC): Cross-platform version of the remote desktop protocol for remote user GUI access. **Use Port 5900**

Remote Access Service:

1. **Password Authentication Protocol (PAP):** Used to provide authentication but is not considered secure since it transmits the login credentials unencrypted (in the clear).
2. **Challenge Handshake Authentication Protocol (CHAP):** Used to provide authentication by using the user's password to encrypt a challenge string of random numbers.



Virtual Private Networks (VPN): Allows end users to create a tunnel over an untrusted network and connect remotely and securely back into the enterprise network.

VPN Concentrator: Specialized hardware device that allows for hundreds of simultaneous VPN connections for remote workers.

Split Tunneling: A remote worker's machine diverts internal traffic over the VPN but external traffic over their own internet connection.

RADIUS vs TACAS:

Remote Authentication Dial-In User Service (RADIUS): Provides centralized administration of dial-up, VPN and wireless authentication services for 802.1x and the Extensible Authentication Protocol (EAP). **Use UDP**

- **Port 1812** or **1645** for **Authentication.**
- **Port 1813** or **1646** for **Accounting.**

- **Cisco's TACACS+** is a proprietary version of RADIUS. **Port 49 (TCP)**

Access Control:

Access Control: Methods used to secure data and information by verifying a user has permissions to read, write, delete, or otherwise modify it.

Access Control Models:

1. **Discretionary Access Control (DAC):** The access control policy is determined by the owner.
2. **Mandatory Access Control (MAC):** An access control policy where the computer system determines the access control for an object.
   a. **Rule-based Access Control:** Label-based access control that defines whether access should be granted or denied to objects by comparing the object label and the subject label.
   b. **Lattice-based Access Control:** Utilizes complex mathematics to create sets of object and subjects to define how they interact.
3. **Role-based Access Control (RBAC):** An access model that is controlled by the system (like MAC) but utilizes a set of permissions instead of single data label to define the permission level.
4. **Attribute-Based Access Control (ABAC):** An access model that is dynamic and context-aware using IF-THAN statements.

Best Practice:

1. **Implicit Deny:** All access to a resource should be denied by default and only be allowed when explicitly stated.
2. **Least Privilege:** Users are only given the lowest level of access needed to perform their job functions.
3. **Separation of Duties:** Requires more than one person to conduct a sensitive task or operation.
4. **Job Rotation:** Occurs when users are cycled through various jobs to learn the overall operations better, reduce their boredom, enhance their skill level, and most importantly, increase our security.

Users and Groups:

- **User Rights:** Permissions assigned to a given user.
- **Groups:** Collection of users based on common attributes (Generally work roles).

- **chmod:** Program in Linux that is used to change the permissions or rights of a file or folder using a shorthand number system.
    - **Read= 4**
    - **Write= 2**
    - **Execute= 1**
- **Privilege Creep:** Occurs when a user gets additional permission over time as they rotate through different positions or roles.
- **User Access Recertification:** Process where each user's rights and permissions are revalidated to ensure they are correct.

- **Propagation:** Occurs when permissions are passed to a subfolder from the parent through inheritance.
- **Strong Passwords:** Contain uppercase letters, lowercase letters, numbers, special characters, and at least 8 characters or more.

User Account Control (UAC): A security component in windows that keeps every user in standard user mode instead of acting like an administrative user.

Risk Management:

<u>Risk Assessment</u>: A process used inside of risk management to identify how much risk exists in a given network or system.

<u>Risk</u>: The probability that a threat will be realized.

<u>Vulnerabilities</u>: Weaknesses in the design or implementation of a system. (it is internal we can control it)

<u>Threat</u>: Any condition that could cause harm, loss, or damage to our information technology systems. (it is external so we can just minimize it)

Strategy to deal with risk:

1. **Risk Avoidance:** A strategy that requires stopping the activity that has risk or choosing a less risky alternative.
2. **Risk Transfer:** A strategy that passes the risk to a third party.
3. **Risk Mitigation:** A strategy that seeks to minimize the risk to an acceptable level.
4. **Risk Acceptance:** A strategy that seeks to accept the current level of risk and the costs associated with it if the risk were realized.
5. **Residual Risk:** The risk remaining after trying to avoid, transfer, or mitigate the risk.

- **Qualitative analysis** uses intuition, experience, and other methods to assign a relative value to risk.
- **Quantitative analysis** uses numerical and monetary values to calculate risk.
- **Hybrid approaches** that combine Quantitative analysis and Qualitative analysis are commonly used.

Magnitude of Impact or Risk Impact: An estimation of the amount of damage that a negative risk might achieve.

Three most common calculation used in Quantitative analysis:

1. **Single Loss Expectancy (SLE):** Cost associated with the realization of each individualized threat that occurs. (**SLE= Asset Value * Exposure Facto**)
2. **Annualized Rate of Occurrence (ARO):** Number of times per year that threat is realized.
3. **Annualized Loss Expectancy (ALE):** Expected cost of a realized threat over a given year. (**ALE= SLE * ARO**)

Security Assessments: Verify that the organization's security posture is designed and configured properly to help thwart different types of attack.

- **Active Assessments:** Utilize more intrusive techniques like scanning, hands-on testing, and probing of the network to determine vulnerabilities.
- **Passive Assessments:** Utilize open secure information, the passive collection and analysis of the network data, and other unobtrusive methods without making direct contact with the targeted systems.

Security Controls: Methods implemented to mitigate a particular risk.

1. **Physical Controls:** Any security measures that are designed to deter or prevent unauthorized access to sensitive information or the systems that contain it.
2. **Technical Controls:** Safeguards and countermeasures used to avoid, detect, counteract, or minimize security risks to our systems and information.
3. **Administrative Controls:** Focused on changing the behavior of people instead of removing the actual risk involved.

NIST categories:

1. **Management Controls:** Security controls that are focused on decision-making and the management of risk.
2. **Operational Controls:** Focused on the things done by people.
3. **Technical Controls:** Logical controls that are put into a system to help secure it.

Other categories:

1. **Preventative:** Security controls that are installed before an event happens and are designed to prevent something from occurring.
2. **Detective Controls:** Used during the event to find out whether something bad might be happening.
3. **Corrective Controls:** Used after event occurs.

Compensating Control: Used whenever you can't meet the requirement for a normal control.

- **Residual risk** not covered by a compensating control is an accepted risk.

Vulnerability Assessment: Seeks to identify any issues in a network, application, database, or other systems prior to it being used that might compromise the system.

Vulnerability Management: Practice of finding and mitigating the vulnerabilities in computers and networks.

Pivot: Occurs when an attacker moves onto another workstation or user account.

Persistence: Ability pf an attacker to maintain a foothold inside the compromised network.

Open Vulnerability and Assessment Language (OVAL): A standard designed to regulate the transfer of secure public information across network and the internet utilizing any security tools and services available.

- **OVAL Language:** An XML schema used to define and describe the information being created by OVAL to be shared among the various programs and tools.
- **OVAL Interpreter:** A reference developed to ensure the information passed around by these programs complies with the OVAL schemas and definitions used by the OVAL language.

Vulnerability Assessment: Baselining of the network to assess the current security state of computers, servers, network devices, and the entire network in general.

- **Network Mapping:** Discover and documentation of physical and logical connectivity that exists in the network.
- **Vulnerability Scanning:** A technique that identifies threats on the network without exploiting them.
- **Banner Grabbing:** A technique used to gain information about servers and inventory the systems or services.
- **Network Sniffing:** The process of finding and investigating other computers on the network by analyzing the network traffic or capturing the packets being sent.
- **Protocol Analyzer:** Software tool that allows for the capture, reassembly, and analysis of packets from the network.

Password Analysis: A tool used to test the strength of your passwords to ensure your password policies are being followed.

Password Cracker: Uses comparative analysis to break passwords and systematically continues guessing until the password is determined.

Password Cracking Methods:

1. **Password Guessing:** Occurs when a weak password is simply figured out by a person.
2. **Dictionary Attack:** Method where a program attempts to guess the password by using a list of possible passwords.
3. **Brute-Force Attack:** Method where a program attempts to try every possible combination until it cracks the password.
4. **Cryptanalysis Attack:** Comparing a precomputed encrypted password to a value in a lookup table.

Rainbow Table: List of precomputed valued used to more quickly break a password since values don’t have to be calculated for each password being guessed.

Monitoring and Auditing:

1. **Signature-based:** Network traffic is analyzed for predetermined attack patterns.
2. **Anomaly-based**: A baseline is established and any network traffic that is outside of the baseline is evaluated.
3. **Behavior-based:** Activity is evaluated based on the previous behavior of applications, executables, and the operating system in comparison to the current activity of the system.

Baseline: Process of measuring changes in networking, hardware, software, and applications.

Baseline Reporting: Documenting and reporting on the changes in a baseline.

Security Posture: Risk level to which a system or other technology element is exposed.

Protocol Analyzer ca connect to your network in:

1. **Promiscuous mode:** Network adapter is able to capture all of the packets on the network regardless of the destination MAC address of the frames carrying them.
2. **Non- Promiscuous mode:** Network adapter can only capture the packets addressed to itself directly.

Port Mirroring: One or more switch ports are configured to forward all of their packets to another port on the switch.

Network Tap: A physical device that allows you to intercept the traffic between two points on the network.

Simple Network Management Protocol (SNMP): A TCP/IP protocol that aids in monitoring network-attached devices and computers.

SNMP has Three components:

1. **Managed Devices:** Computers and other network-attached devices monitored through the use of agents by a network management system.
2. **Agent:** Software that is loaded on a managed device to redirect information to the network management system.
3. **Network Management System (NMS):** Software run on one or more servers to control the monitoring of network-attached devices and computers.

Logs: Data files that contain the accounting and audit trail for actions performed by a user on the computer or network.

Three types of Logs in Windows:

1. **Security Logs:** Logs the events such as successful and unsuccessful user logons to the system.
2. **System Logs:** Logs the events such as a system shutdown and driver failures.
3. **Application Logs:** Logs the events for the operating system and third-party applications.

SYSLOG: A standardized format used for computer message logging that allows for the separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. (Use **Port 514** over **UDP**)

Log File Maintenance: Actions taken to ensure the proper creation and storage of a log file, such as the proper configuration, saving, backing up, securing, and encrypting of the log file.

Overwrite Events: When a maximum log size is reached, the system can begin overwriting the oldest event I the log files to make room.

Write Once Read Many (WORM): Technology like a DVD-R that allows data to be written only once but read unlimited times.

Security information and Event Management (SIEM): Combines security event management and security information management systems into one tool.

Data Aggregation: Combines data from various network devices, servers, and applications from across the enterprise network.

Data Correlation: Automatically looks for common attributes of events across the monitored portions of the network.

Cryptography:

Cryptography: The practice and study of writing and solving codes in order to hide the true meaning of information.

Encryption: Process of converting ordinary information (plain text) into unintelligible form (ciphertext).

Data at Rest: Inactive data that is archived such as data resident on a hard disk drive.

Data in Transit: Data crossing the network or data that resides in a computer's memory.

Data in Use: Data that is undergoing constant change.

Key: The essential piece of information that determines the output of cipher.

- **Symmetric Algorithm (Private Key):** Encryption algorithm in which both the sender and the receiver must know the same secret using a privately held key. (Do not achieved Non-Repudiation)
  1. **Data Encryption Standard (DES):** Encryption algorithm which breaks the input into 64-bit blocks and uses transposition and substitution to create ciphertext using an effective key strength of only 56-bits.
  2. **Triple DES (3DES):** Encryption algorithm uses three separate symmetric keys to encrypt, decrypt, then encrypt the plaintext into ciphertext in order to increase the strength of DES.
  3. **International data Encryption Algorithm (IDEA):** Symmetric blocks cipher which uses 64-bit blocks to encrypt plaintext into ciphertext.
  4. **Advanced Encryption Standard (AES):** Symmetric block cipher that uses 128-bit, 192-bit, or 256-bit blocks and matching encryption key size to encrypt plaintext into ciphertext.
  5. **Blowfish:** Symmetric block cipher that uses 64-bit block and a variable length encryption key to encrypt plaintext into ciphertext.
  6. **Towfish:** Symmetric block cipher that replaced blowfish and uses 128-bit block and a 128-bit, 192-bit, or 256-bit encryption key to encrypt plaintext into ciphertext.

- **Asymmetric Encryption (Public Key):** Encryption algorithm where different keys are used to encrypt and decrypt the data.
    1. **Diffie-Hellman (DH):** Used to conduct key exchanges and secure key distribution over an unsecure network. (used for establishment a **VPN** tunnel using **IPSec**)
    2. **RSA:** Asymmetric algorithm that relies on the mathematical difficulty of factoring large prime numbers. (it can use key size of 1024-bit to 4096-bit)
    3. **Elliptic Curve Cryptography (ECC):** Algorithm that is based upon the algebraic structure of elliptic curves over finite fields to define the keys. (used for mobiles and low-power devices)
- **Hybrid Implementation:** Utilizes asymmetric encryption to securely transfer a private key that can then be use with symmetric encryption.

Stream Cipher: Utilizes a keystream generator to encrypt data bit by bit using a mathematical XOR function to create the ciphertext. (Symmetric)

Block Cipher: Breaks the input into fixed-length blocks of data and performs the encryption on each block.

- Note: in all symmetric examples **RC4** is the only **Stream cipher, Else** is **block cipher.**

Digital Signature: A hash digest of a message encrypted with the sender's private key to let the recipient know the document was created and sent by the person claiming to have sent it.

Pretty Good Privacy (PGP): An encryption program used for signing, encrypting, and decrypting emails.

GNU Privacy Guard (GPG): A newer and updated version of the PGP encryption suite that uses AES for its symmetric encryption functions.

Key Management: Refers to how an organization will generate, exchange, store, and use encryption key.

One-Time Pad: A stream cipher that encrypts plaintext information with a secret random key that is the same length as the plaintext input.

Pseudo-Random Number Generator (PRNG): A simulated random number stream generated by computer that is used in cryptography, video games, and more.

- For encode and decode in steganography use http://stylesuxx.github.io/steganography/

Hashing: A one-way cryptographic function which takes an input and produces a unique message digest.

1. **Message Digest 5 (MD5):** Algorithm that creates a fixed-length 128-bit hash value unique to the input file.
2. **Secure Hash Algorithm (SHA).**
3. **RACE Integrity Primitive Evaluation Message Digest (RIPEMD):** An open-secure hash algorithm that creates a unique 160-bit, 256-bit, or 320-bit message digest for each input file.
4. **Hash-based Message Authentication Code (HMAC):** Uses a hash algorithm to create a level of assurance as to the integrity and authenticity of a given message of file.

5. **Code Signing:** Uses digital signatures to provide an assurance that the software code has not been modified after it was submitted by the developer.
6. **LANMAN (LM Hash):** Original version of password hashing used by Windows that uses DES and is limited to 14 characters.

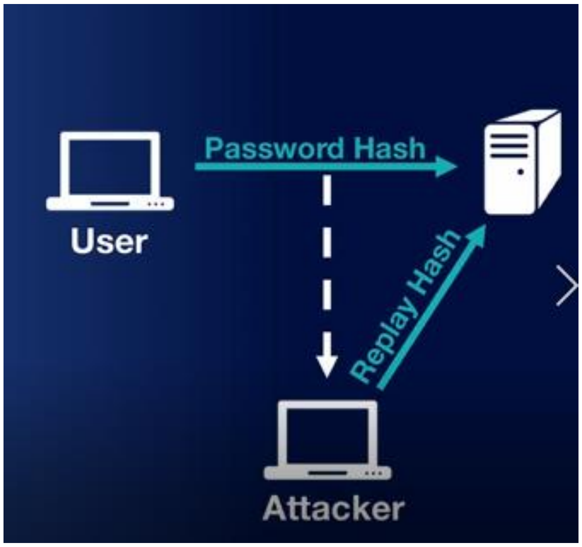
Collision: Condition that occurs when two different files create the same hash digest.

Note: Hash is used to ensure Integrity, and **MD5** and **SHA** is the most common hash functions used.

- For Hashing use https://passwordsgenerator.net/md5-hash-generator/

Hash Functions:

1. **Pass the Hash:** A technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLN or LM hash instead of requiring the associated plaintext password.



Pen Test tool: **Mimikatz:** A Penetration testing tool used to automate the harvesting of hashes and conducting the pass the hash attack.

2. **Birthday Attack:** Technique used by the attacker to find two different messages that have the same identical hash digest.

Increasing Hash Security:

1. **Key Stretching:** A technique used to mitigate a weaker key by increasing the time needed to crack it.
2. **Salting:** Adding random data into a one-way cryptography hash to help protect against password cracking technique.

Public key Infrastructure (PKI)

Public key Infrastructure (PKI): An entire system of hardware, software, policies, procedures, and people that is based on asymmetric encryption.

Certificates: Digitally-signed electronic documents that bind a public key with a user's identity.

X.509: Standard used PKI for digital certificates and contains the owner/users information and the certificate authority's information.

Wildcard Certificates: Allows all of the subdomains to use the same public key certificate and have it displayed as valid. (easier to manage)

Subject Alternative Name (SAN): Allows a certificate owner to specify additional domains and IP addresses to be supported.

- **X.690** uses **BER**, **CER**, and **DER** for encoding.

1. **Basic Encoding Rules (BER):** The original ruleset governing the encoding of data structures for certificates where several different encoding types can be utilized.
2. **Canonical Encoding Rules (CER):** A restricted version of the BER that only allows the use of only one encoding type.
3. **Distinguished Encoding Rules (DER):** Restricted version of the BER which allows one encoding type and has more restrictive rules for length, character strings, and how elements of a digital certificate are stored in X.509.

- **Privacy-enhanced Electronic Mail:** .pem, .cer, .crt or .key.
- **Public Key Cryptographic System #12 (PKCS#12):** .p12.
- **Personal Information Exchange:** .pfx.
- **Public Key Cryptography Systems #7 (PKCS#7):** .p7b.

Registration Authority (RA): Used to verify information about a user prior to requesting that a certificate authority issue the certificate.

Certificate Authority: The entity that issues certificates to a user.

Certificate Revocation List (CRL): An online list of digital certificates that the certificate authority has revoked.

Online Certificate Status Protocol (OCSP): A protocol that allows you to determine the revocation status of a digital certificate using its serial number.

OCSP Stapling: Allows the certificate holder to get the OCSP record from the server at regular intervals and include it as part of the SSL or TLS handshake.

Public Key Pinning: Allows an HTTPS website to resist impersonation attacks by presenting a set of trusted public keys to the user's web browser as part of the HTTP header.

Key Escrow: Occurs when a secure copy of a user's private key is held in case the user accidently loses their key.

Key Recovery Agent: A specialized type of software that allows the restoration of a lost or corrupted key to be performed.

Web of Trust: A decentralized trust model that addresses issues associated with the public authentication of public keys within a CA-based PKI system.

Security Protocols

Secure/Multipurpose Internet mail Extensions (SMIME): A standard that provides cryptographic security for electronic messaging.

Secure Socket Layer (SSL)/ Transport Layer Security (TLS): Cryptographic protocols that provide secure internet communications for web browsing, instant messaging, email, VoIP, and many other services.

Downgrade Attack: A protocol is tricked into using a lower quality version of itself instead of a higher quality version.

Secure Shell (SSH): A protocol that can create a secure channel between two computers or network devices to enable one device to control the other device. **(Port 22,** and it use Diffie-Hellman key**)**

Virtual Private Networks (VPN): A secure connection between two or more computers or device that are not on the same private network.

1. **Point-to-Point Tunneling Protocol (PPTP):** A protocol that encapsulates PPP packets and ultimately sends data as encrypted traffic. (**Port 1723,** and it use CHAP-based authentication)
2. **Layer 2 Tunneling Protocol (L2TP):** A connection between two or more computers or device that are not on the same private network. (**Port 1701,** it is usually paired with IPSec)
    a. **IPSec:** A TCP/IP protocol that authenticates and encrypts IP packets and effectively securing communications between computers and devices using this protocol.
    b. **Internet Key Exchange (IKE):** Method used by IPSec to create a secure tunnel by encrypting the connection between authenticated peers.
    c. **Security Association (SA):** Establishment of secure connections and shared security information using certificates or cryptographic keys.
    d. **Authentication Header (AH):** Protocol used in IPSec that provides integrity and authentication.
    e. **Encapsulating Security Payload (ESP):** Provides integrity, confidentiality, and authenticity of packets by encapsulating and encrypting them.

IPSec has two Mode:

1. **Transport Mode:** Host-to-host transport mode only uses encryption of the payload of an IP packet but not its header. (used for transmission between hosts on a private network)
2. **Tunnel Mode:** A network tunnel is created which encrypts the entire IP packet (payload and header). (it is commonly used for transmission between networks)

Planning for the Worst

Redundancy: when you have something extra or unnecessary.

Single Point of Failure: The individual elements, objects, or parts of a system that would cause the whole system to fail if they were to fail.

Redundant Power Supply: An enclosure that provides two or more complete power supplies.

- **Surge:** An unexpected increase in the amount of voltage provided.
- **Spike:** A short transient in voltage that can be due a short circuit, tripped circuit breaker, power outage, or lighting strike.
- **Sag:** An unexpected decrease in the amount of voltage provided.
- **Brownout:** Occurs when the voltage drops low enough that it typically causes the lights to dim and can cause a computer to shut off.
- **Blackout:** Occurs when there is a total loss of power for a prolonged period.

Backup Power:

1. **Uninterruptible Power Supply (UPS):** Combines the functionality of a surge protector with that of a battery backup.
2. **Backup Generator:** An emergency power system used when there is an outage of the regular electric grid power.

To Ensure Data Redundancy:

Redundant Array of Independent Disks (RAID): Allows the combination of multiple physical hard disks into a single logical hard disk drive that is recognized by the operating system.

a. **RAID 0:** Provides data striping across multiple disks to increase performance.
b. **RAID 1:** Provides redundancy by mirroring the data identically on two hard disks.
c. **RIAD 5:** Provides redundancy by striping data and parity data across the disk drives.
d. **RIAD 6:** Provides redundancy by striping and double parity data across the disk drives.
e. **RAID 10:** Creates a striped RAID of two mirrored RAIDs. (combines RAID 1 & RAID 0)

1. **Fault-resistant RAID:** Protects against the loss of the array's data a single disk fails (RAID 1 or RAID 5).
2. **Fault-tolerant RAID:** Protects against the loss of the array's data if a single component fails (RAID 1, RAID 5, RAID 6).
3. **Disaster-tolerant RAID:** Provides two independent zones with full access to the data (RAID 10).

Server Redundancy:

Cluster: Tow or more servers working together to perform a particular job function.

1. **Failover Cluster:** A secondary server can take over the function when the primary one fails.
2. **Load-balancing Cluster:** Servers are clustered in order to share resources such as CPU, RAM, and hard disks.

Redundant Sites:

1. **Hot Site:** A near duplicate of the original site of the organization that can be up and running within minutes.
2. **Warm Site:** A site that has computers, phones, and servers but they might require some configuration before users can start working.
3. **Cold Site:** A site that has tables, chairs, bathrooms, and possibly some technical times like phones and network cabling.

Data Backup:

1. **Full Backup:** All of the contents of a drive are backed up.
2. **Incremental Backup:** Only conducts a backup of the content of a drive that have changed since the last full or incremental backup.
3. **Differential Backup:** Only conducts a backup of the contents of a drive that has changed since the last full backup. (take more time to create but less time to restore)

Tape Rotation:

1. **10 Tape Rotation:** Each tape is used once per day for two weeks and then the entire set is reused.
2. **Grandfather-Father-Son:** Three sets of backup tapes are defined as the son (daily), the father (weekly), and the grandfather (monthly).
3. **Towers of Hanoi:** Three sets of backup tapes (like the grandfather-father-son) that are rotated in a more complex system.

Disaster Recovery Planning: The development of an organized and in-depth plan problems that could affect the access of data or the organization's building.

Social Engineering

Social Engineering: Manipulates a user into revealing confidential information that are detrimental to the user or the security of our system.

Insider Threat: A person who works for or with your organization but has ulterior motives.

- **Phishing:** An attempt to fraudulently obtain information from a user (usually by email).
- **Smishing:** Phishing conducted over text messaging (SMS).
- **Vishing:** Phishing conducted over voice and phone calls.
- **Pharming:** Phishing attempt to trick a user to access a different or fake website (usually by modifying hosts file).

➢ **Diversion Theft:** When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location.

➢ **Hoax:** Attempt at deceiving people into believing that something is false when it is true (or vice versa).

➢ **Shoulder Surfing:** When a person uses direct observation to obtain authentication information.

➢ **Eavesdropping:** When a person uses direct observation to "listen" into a conversation.

➢ **Dumpster Diving:** When a person scavenges for private information in garbage containers.

➢ **Baiting:** When a malicious individual leaves malware-infected removable media such as a USB or optical disc lying around in plain view.

➢ **Piggybacking:** When an unauthorized person to gain entry to a restricted area.

➢ **Watering Hole Attack:** When an attacker figures out where users like to go, and places malware to gain access to your organization.

Clean Disk Policy: Policy where all employees must put away everything from their desk at the end of the day into locked draws and cabinets.

Policies and Procedures

1. **Policies:** Defines the role of security in an organization and establishes the desired end state of the security programs.
2. **Organizational Policies:** Provide general direction and goals, a framework to meet the business goals, and define the roles, responsibilities, and terms.

3. **System-Specific Policies:** Address the security needs of a specific technology, applications, network, or computer system.
4. **Issue-Specific Policies:** Built to address a specific security issue, such as email privacy, employee termination procedures, or other specific issues.

Baseline: Created as reference points which are documented for use as a method of comparison during an analysis conducted in the future.

Procedures: Detailed step-by-step instructions that are created to ensure personnel can perform a given action.

- Policies are generic.
- Procedures are specific.

Data Classification: Category based on the value to the organization and the sensitivity of the information if it were to be disclosed.

Sensitive Data: Any information that can result in a loss of security, or loss of advantage to a company, if accessed by unauthorized persons.

Tow classification based on organization if it was commercial or government:

1. **Commercial:**
    a. **Public:** Has no impact to the company if released and is often posted in the open-source environment.
    b. **Sensitive:** Might have a minimal impact of released.
    c. **Private:** Contains data that should only be used within the organization.
    d. **Confidential:** Highest classification level that contains items such as trade secrets, intellectual property data, source code, and other types that would seriously affect the business if disclosed.
2. **Government:**
    a. **Unclassified:** Can be released to the public.
    b. **Sensitive But Unclassified:** Items that wouldn't hurt national security if released but could impact those whose data is contained in it.
    c. **Confidential Data:** Data that could seriously affect the government if unauthorized disclosure were to happen.
    d. **Secret Data:** Data that could seriously damage national security if disclosed.
    e. **Top Secret Data:** Data that could gravely damage national security if it were known to those who are not authorized for this level of information.

Personal identifiable Information (PII): A piece of data that can be used either by itself or in combination with some other pieces of data to identify a single person.

Lows you should know:

1. **Privacy Act of 1974:** Affects U.S. government computer systems that collects, stores, uses, or disseminates personally identifiable information.
2. **Health Insurance Portability and Accountability Act (HIPAA):** Affects healthcare providers,

facilities, insurance companies, and medical data clearing houses.

3. **Sarbanes-Oxley (SOX):** Affects publicly-traded U.S. corporations and requires certain accounting methods and financial reporting requirements.
4. **Gramm-Leach-Bliley Act (GLABA):** Affects banks, mortgage companies, loan offices, insurance companies, investment companies, and credit card providers.
5. **Federal Information Security Management (FISMA) Act of 2002:** Requires each agency to develop, document, and implement an agency-wide information systems security program to protect their data.
6. **Help America Vote Act (HAVA) of 2002:** Provides regulations that govern the security, confidentiality, and integrity of the personal information collected, stored, or processed during the election and voting process.

Acceptable Use Policy: Defines the rules that restrict how a computer, network, or other system may be used.

Change Management Policy: Defines the structured way of changing the state of a computer system, network, or IT procedure.

Job Rotation: Different users are trained to perform the tasks of the same position to help prevent and identify fraud that could occur if only one employee had the job.

Onboarding and Offboarding Policy: Dictates what type of things need to be done when an employee is hired, fired, or quits.

Concept keep in your mind when you write the policies:

1. **Due Diligence:** Ensuring that IT infrastructure risks are known and managed properly.
2. **Due Care:** Mitigation actions that an organization takes to defend against the risks that have been uncovered during due diligence.
3. **Due Process:** A legal term that refers to how an organization must respect and safeguard personnel's rights.

User Education:

1. **Security Awareness Training:** Used to reinforce to users the importance of their help in securing the organization's valuable resources.
2. **Security Training:** Used to teach the organization's personnel the skills they need to perform their job in a more secure manner.
3. **Specialized Training:** May be developed too.

Vendor Relationships:

1. **Non-Disclosure Agreement (NDA):** Agreement between two parties that defines what data is considered confidential and cannot be shared outside of the relationship.
2. **Memorandum of Understanding (MOU):** A non-binding agreement between two or more organization's to detail an intended common line of action.
3. **Service-Level Agreement:** An agreement concerned with the ability to support and respond to problems within a given timeframe and continuing to provide the agreed upon level of service to the user.

4. **Interconnection Security Agreement (ISA):** An agreement for the owners and operations of the IT systems to document what technical requirements each organization must meet.
5. **Business Partnership Agreement (BPA):** Conducted between two business partners that establishes the conditions of their relationship.

Disposal Policies:

- **Degaussing:** Exposes the hard drive to a powerful magnetic field which in turn causes previously-written data to be wiped form the drive.
- **Purging (Sanitizing):** Act of removing data in such a way that it cannot be reconstructed using any known forensic techniques.
- **Clearing:** Removal of data with a certain amount of assurance that it cannot be reconstructed.

Incident Response Procedures:

Incident Response: A set of procedures that an investigator follows when examining a computer security incident.

Incident Management Program: Program consisting of the monitoring and detection of security events on a computer network and the execution of proper responses to those security events.

Identification: Process of recognizing whether an event that occurs should be classified as an incident.

Recovery: Focused on data restoration, system repair, and re-enabling any servers or networks taken offline during the incident response.

IT Security Framework:

1. Sherwood Applied Business Security Architecture (SABSA).
2. Control Objectives for Information and Related Technology (COBIT).
3. NIST SP 800-53.
4. ISO 27000.
5. ITIL.

Good Luck