Data Classification

- Roles
    - Data Owner: Classifies Data and approves level of access
    - Data Custodian: configures the level of access and backs up data
    - Privacy Officer: Ensures that appropriate privacy laws are followed
- Types of Classifications
    - 2 Systems
        - Commercial
            - Confidential - Trade secrets, code, healthcare information
            - Private - salaries
            - Sensitive - financial info, profits, projects
            - Public - common knowledge
        - Military
            - Top-secret
            - Secret
            - Confidential
            - Sensitive but unclassified
    - Others:
        - Proprietary Information
            - Trade secrets, formulas
                - Used for corporate espionage, the act of stealing proprietary information for the intent of selling it or blackmailing the company

Authentication Management

- Static KBA (Knowledge Based Access)
    - Windows Questions: when you set up a computer (where were you born?)
- Dynamic KBA
    - Clash Royale: What was the last card you upgraded?
- Password Key
    - A password that can both unlock and lock something
- Password Vault
    - LastPass, Google Passwords, Apple Passwords

Data Types and Privacy Protection

- 2 Types of protected data
    - PII: Age, Name, DOB, SSN
    - PHI: health records

Code Based Attacks

- Improper input handling vs error handling

    - Input is more of validation, sanitation, and restrictions, susceptible to buffer overflows, SQL injections, and XSS
    - Error Handling is more of responding to issues like, server unavailable
- Configurations
    - Never use the default configuration with default usernames and passwords
- Stored Procedures
    - Series of SQL statement that are executed as a group, similar to a script
- Input Validation
    - Every input is validated against a range of acceptable values

Provisioning

- Removing and adding resources based on current demand for those resources

Network Service Attacks

- Packet Sniffers: Promiscuous mode scans through all cleartext data in a network environment
- SYN Floods: A spoofed IP address sends out SYN packets to a host server, and it tries to respond with a large amount of ACK packets, wasting resources and shutting down
- Known Plaintext: When someone knows the cipher key given a couple of examples and can decrypt the rest of the data
- Traffic Analysis: technique used to analyze network traffic, such as message lengths and frequency

Wireless Attacks

- Bluetooth
    - Bluesnarfing: gain control
    - Bluejacking: send a message
- War Driving
    - Driving around with a laptop to discover unprotected networks
- Spamming
    - Sending unsolicited emails through a mail server
- NFC
- Replay Attacks
- WPS Attacks (Wifi Protected Setup)

Installation and Configuration

- Wireless Access Points
    - Fat: Standalone and manual configuration, do not change until they die
    - Thin: Configuration from a switch or router, dynamic
    - Controller: configure remotely amd no manual config

    - Standalone: has its own management interface
- Isolation mode
    - Wireless clients can only communicate with the WAP and not with other wireless clients
- PEAP (Protected Extensible Authentication Protocol)
    - Secure password based authentication protocol created to simplify secure authentication
- SSID (service set identifier)
    - Wireless network's name
- LEAP (lightweight Extensible Authentication Protocol)
    - Authentication protocol by Cisco

Network Appliances

- IDS (Intrusion Detection Systems)
    - Anomaly Based: catches deviations in normal traffic/behavior
    - Signature Based: catches deviation in well known malware
    - Behavior Based: catches deviation based on set rules
    - Misuse-detection Based: same as signature
- Load Balancers
    - Balance load between web servers
- SSL Accelerators
    - Assist the processor intensive activities associated with SSL/TSL encryption
- Software Defined Network (SDN)
    - Virtualizes the entire network , including the security devices
- DDoS Mitigator
    - Placed on the perimeter network, detects and mitigates DDoS attacks
- Aggregation switches
    - Create a single bandwidth dream from multiple sources
- Correlation Engines
    - Examine logs from several firewalls and aggregate the entire to determine attack patterns
- VPN Concentrators
    - Need to be placed near the edge or gateway of a network

- Hub
    - Device that connects multiple ethernet connections, making them act as a single network segment. .
    - Connects hosts on a network; CANNOT configure ACLs
- Firewalls

        - Monitors and controls incoming and outgoing network traffic based on predetermined security rules
- Router
    - Forwards data packets between computer networks.
    - Directs traffic on the internet and within a home
    - “Connects devices within a home to internet”
- Modems
    - Connect networks to the internet
    - Cannot manage internal data traffic
    - “Modem to ISP”

Personnel

- Vacations CAN lower breach incidents. Roles can be reassessed and the replacement employee can notify if something unusual is happening with the other employee
- NDAs CANNOT guarantee a lower chance of breach.

IP Addresses

- Understand Bits and Bytes
    - One Byte is 8 Bits
    - Each Bit is a 0 or 1
    - 8 Bits can equal a max of 256 or minimum of 0
- The first 4 bits of an IP header is the version. IPv4 is 0010 and IPv6 os 0110
- IPv6 addresses CAN BE 4 times longer than IPv4 addresses, but their headers are only 2 times longer

GRC

- A legal hold mandates that a company not change remove or add anything to their systems while legal actions are being held
- A chain of custody is vital for preserving integrity and keeping track of who touched the data and when
- Data Sovereignty ensures that data from one country stays in the country it is being stored in

Encryption

- (reversible unlike hashing)
- Asymmetric
    - Uses a public and private key to encrypt and decrypt
    - **Vulnerable to new quantum computing efforts**
    - RSA for secure data transmission
- One-Way Encryption

  - Encrypts data in a way that cannot be reversed, password hashing
  - SHA-256 for securing passwords
- Symmetric Encryption
  - Uses the same key for encryption and decryption
  - AES (Advanced Encryption Standard) for data at rest
- Lattice Based Encryption
  - Based on lattice problems
  - NTRU, a candidate for post-quantum cryptography

- ECC (Elliptic Curve Cryptography)
  - More efficient and uses less resources than RSA

- BitLocker to Go
  - Use this for USB Portable Drives
- Data Encryption Standard
  - Algorithm for data transmission, similar to AES
- Encrypting File System (EFS)
  - Encrypts individual files, not entire drives
  -

Mobile Devices and Connection Methods

- Printers, and other multifunctional devices use Telnet
- Wireless keyboards and mice can be spoofed and remotely controlled
- Any other wifi enabled device should be scanned periodically for malware

Access Control

- RBAC: using user groups and their assigned roles to give permissions
- ABAC: using where and when someone is accessing to manage permissions

Systems

- Embedded: a device with its own proprietary software and hardware; a mini-brain
- Black Box: anything where you just use the device without question of what's inside

Web Attacks

- M-i-t-Broswer Attacks
  - An attacker redirects your website to a malicious one
- MitMiddle Attack
  - An attacker intercepts and changes the data you're sending over internet
- Session Hijacking
  - An attacker eavesdrops on a conversation

- Remote Access Trojan
    - A backdoor is installed instead of a legit application

MITRE Attack Framework

- A curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

IoT Devices

- Unmanned Aerial Vehicles
    - Drones, or other flying things without a human inside
- Wearable Technologies
    - Voice recorders, smart watches, video recorders, cameras can all be intercepted
    - Medical Devices

DAST and SAST

- Dynamic and Static Application Sec Testing should be used on all applications during their development

Qualitative Risk Analysis

- Decision Tree
    - Tree like model of decisions and their possible consequences
- Monte Carlo
    - Risk management technique, where PMs use the impacts of various risks on the projects cost and project timeline
- Pareto Principle
    - 80% of consequences come from 20% of the causes
- Delphi Technique
    - Experts fill out anonymous questionnaires, which keeps one or more experts from dominating a conversation

Other Attacks

- Data Diddling
    - Changing data for financial gain
- Sniffing
    - You CAN sniff out a password if its being transferred in cleartext
- Privilege Escalation
    - Gaining addition privileges beyond what is expected
- Resource Exhaustion
    - Computer parts are overleveraged
- Directory Traversal

    - Using an application to find where it has access to and move around directories using that information
- Pharming
    - Web Browser; redirects traffic to a bogus site
- Xmas
    - Port scan for open ports
- Vishing
    - Discover financial or other private information via phone
- Spimming
    - Pretending to be a friend of a victim to send a nefarious message

Firewalls

- Software firewall
    - Software, not hardware
- Hardware firewall
    - “Appliance Firewall”
    - Standalone black box solutions that can be plugged into a network without much configuration
- Application firewall
    - Integrated into another type of firewall, such as a hardware firewall
- Embedded Firewall
    - Implemented as a component of a hardware device, such as a switch or a router

Roles in a Network Security Team

- Approve Change
    - Network admins can approve changes
- Test Change
    - Vulnerability Management roles can request and test changes
- Request Change
    - Incident Response roles can request changes
- Implement Changes
    - DevOps roles can implement changes through code or engineering

Advanced Persistent Threats (APT)

- Not necessarily malware, but often refers to the group of people that stay stealthy and maintain root access to a network

SKIP (Simple Key management protocol for Internet Protocols)

- Used for secure IP communication, such as IPsec
- Uess hybrid encryption to convey session keys, which are used to encrypt data in IP packets

SLE (Single Loss Expectancy)

- Calculated by multiplying the asset value by its expected loss

DHCP Servers

- APIPA Addresses
    - Start with 169.254.x.x
- When the scope changes, an admin should use the ipconfig /renew and /release commands to update the system

Principle of Least Privilege

- All users should have 1 or more accounts. Administrators should have one normal account and one administrator account.
- Issuing the Run As command to execute administrative tasks during a regular user session IS an example of PoLP

Proxy Servers

- Application Proxy: intercepts all messages entering and leaving a network at the application player of OSI Model
- Multipurpose Proxy: handles multiples types of protocols or services simultaneously
    - Example: an App Proxy might handle HTTP, HTTPS, FTP, and SMTP
- Reverse Proxy: retrieves resources on behalf of a client from one or more servers; these are returned to the client as if it came from the proxy
    - Think of it as a help desk rep who collects all information from managers, notes, and databases and returns to you with everything
    - Also known as a surrogate proxy
        - Think of it as SIR WHO GETS
- Transptercepts all traffic between a client and a server without any configuration
- arent Proxy
    - InUsed for content filtering; user might not even know its there
    - Think of this as a hidden camera that monitors all traffic without people knowing its there.

Threat Websites

- OWASP Top 10
- DHS Automated Indicator Sharing Database
    - Maintains a program that allows orgs to share and obtain machine comprehensible defensive measures and cyber threat indicators
- FBI Infraguard Portal
    - Educational portal for those in the private sector

- US CERT Bulletin
    - Weekly bulletins that summarize new vulnerabilities and possible patch options
    - This is the BIGGEST, most up to date website!
- Microsoft Security Response Center Blog
    - This blog keeps up with the latest threats through updates and authoritative assistance

Tools

- Snort
    - Network intrusion detection system
- Password recovery tool
    - Cain and Abel
- Nessus
    - Vulnerability Scanner
- Wireshark
    - Network Protocol Analyzer

Understand Ports and Protocols

- Ports are where data moves and where it goes
- Protocols are how the data moves, with what rules does it abide by

- Cryptographic communication protocol
    - SSL/TLS
- Secure encryption and digital signatures for email
    - S/MIME
- Routing and Switching Management
    - SNMPv3
- Secure Remote Access
    - SSH
- CHAP (Challenge HandShake Authentication Protocol)
    - Uses a secret password that only both sides know
    - Does not reveal the challenge
    - Challenge goes right, answer goes back, accept/reject response

Cryptographic Techniques

- IV (Initializing Vector)
- Diffusion
    - One change in a input bit results in a change in multiple output bits
- Confusion

    - The components of a message do not match the cipher text
- Salting
    - Adding characters before hashing data

IDS and IPS

- In-Band Out-of-Band
    - Local management vs remote management
- Inline vs Passive
    - Inline monitors and responds immediately
    - Passive just scans and notifies
- Rules define what the IDS/IPS will do in certain scenarios

Hacking Tools

- Metasploit Framework
    - Penetration testing platform that facilitates in the writing, testing, and executing of exploit code and known vulnerabilities
- OWASP ZAP
    - Web application tester (Open Source)
- RainbowCrack
    - For Passwords
- BurpSuite
    - In depth analyzer / web application tester

Risk Mitigation

- Privacy/Screen Filters
    - Privacy screen protectors for laptops and computers
- Airgap
    - Separating insecure networks from secure ones
- Logs
    - Keep track of actions within a system or environment
- Key Management
    - Maintenance of digital certificates, public keys, and private

- Remember that you cannot edit commercial application code, only proprietary. Therefore, to mitigate risk when using 3rd party software, maintain regular updates.

NIST CSF

- Identify: Establishes an understanding of managing cybersecurity risk to systems, assets, data, and capabilities.

- Protect: Outlines safeguards to ensure delivery of critical infrastructure services and limit the impact of potential cybersecurity events.
- Detect: Defines the appropriate activities to identify the occurrence of a cybersecurity event promptly.
- Respond: Focuses on developing and implementing the appropriate activities to take action regarding a detected cybersecurity incident.
- Recover: Details the plans and processes necessary to restore any capabilities or services that were impaired due to a cybersecurity incident.

IPsec

- Host to Gateway
- Gateway to Gateway
- Host to Host

DMZ

- All systems in a DMZ can be accessed from the internet, therefore to keep them safe, you need to implement all computers and firewalls as a bastion host
- A DMZ should have external facing services like servers.
- In a network where both sides of a DMZ needs to be protected from the internet, there must be a firewall on both sides on the DMZ.

Internet Devices

- Routers are used to manage subnets; connect networks toether
- Switches are used to connect devices on a network together
- Modems are a gateway from the internet; converts data from your ISP to be usable

Endpoint Protection

- Faraday Cage
    - A physical room with extreme sound dampening material and expen sive tools that prevent any outside reach of signals, electric, and others. Untappable
- AirGap
    - Separation of secure and insecure networks
- Sandboxing
    - Developing an application or testing outside of a production environment
- Tokens and Cards
    - Physical keys for building and rooms

Disaster Recovery Plan

- Outlines what should happen within a company if a natural disaster were to occur, not a breach.
- Not necessarily needs to be contracted outwards. That would be a “Alternate Processing Site”, which consists of hot, warm, and cold sites

Types of Viruses

- Phase: modifies other programs and databases
- Armored: Includes protective code that is not suspicious on the outside
- Stealth: Hides from applications, file information is not accurate
- Companion: Attaches itself to applications, executes when the app is opened

Syslog Server

- Combines events and other information into a SINGLE congregated log

WiFi Standards

- WPA is backwards compatible and is secure
- WEP is obsolete and not as secure as WPA
- WPA2 is WPA with hardware upgrades
    - WPA2 Enterprise is the most secure standard for businesses
- WAP is a standard for Mobile Phones

Wifi Antenna Placement

- Antennas should be placed as far away from entrances as possible
- Antenna strength should be just enough to reach the front door
- Antenna types should be picked carefully

VLAN

- A type of network that is controlled and restricted, separate from another segment of a large network
- Created by a switch

Secure Web Gateway (SWG)

- Cloud based gateway that combines features of a Next Gen Firewall and a Web Application Firewall

Firewalls

- Packet-Filtering Firewall:
    - Inspects incoming and outgoing packets.
    - Blocks or allows packets based on IP addresses, ports, and protocols.
- Stateful Inspection Firewall:

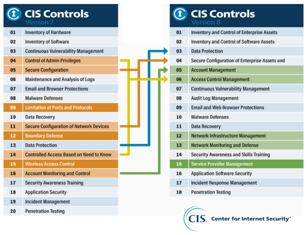
        - Tracks the state of active connections.
        - Makes decisions based on context and state of traffic.
- Proxy Firewall:
    - Intercepts and inspects all messages at the application layer.
    - Acts as an intermediary between end-users and the internet.
- Next-Generation Firewall (NGFW):
    - Combines traditional firewall functions with additional features like deep packet inspection, intrusion prevention, and application awareness.
    - Can enforce security policies at the application level.
- Web Application Firewall (WAF):
    - Specifically protects web applications by filtering and monitoring HTTP traffic.
    - Guards against common web exploits like SQL injection and cross-site scripting (XSS).
- Unified Threat Management (UTM) Firewall:
    - Integrates multiple security features (firewall, antivirus, intrusion detection/prevention, etc.) into a single device.
    - Provides comprehensive security management.

MTBF
- Mean Time Between Failures

Data in Use/Processing Needs to Be
- CIA'ed
    - Encrypted
    - Hashed
    - Access Control

Emails
- From: <email address>
- Received: <tracking information>
    - Use this to find clues of where the email actually originated
- References: < related messages, replies>
- Reply-to: <return address>

Know the CIS Controls



CIS Controls Version 7

01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS. Center for Internet Security®

Questions:

1. A certain set of Infrastructure Equipment in a corporation is no longer receiving security patches.
    a. You should isolate the network
    b. Upgrading hardware will not fix software issues.
2. Someone is processing, analyzing, and storing data. Who is she?
    a. She is the DATA PROCESSOR
    b. The controller determines what to do with data
    c. Custodian determines where the data goes
    d. Data subject is to whom the data belongs
3. Data that is subject to strict compliance standards is
    a. REGULATED, NOT Confidential. Read carefully
4. Monthly reviews of security logs are called
    a. Recurring Reports
5. To ensure a rapid recovery point before rolling out a software update to systems within a company, an employee should
    a. Create a SNAPSHOT, not any type of backups as they take up too much storage
6. If a companies main data center is susceptible to natural disasters, that company should use
    a. OFFSITE BACKUPS, as cloud backups are susceptible to internet outages.
7. XDRs main objective is to detect and respond to multi-vector threats across the IT department
8. ACCESS CONTROL
    a. RBAC is based on roles
    b. DAC is discretionary, meaning its based off the admins preferences
9. Attack Vectors
    a. Client based attacks require installation and configuration
    b. Agentless attacks are online and are done remotely from a server
10. Password Attacks Differentiation
    a. Horizontal: trying the same passwords on different accounts
    b. Dictionary: trying a bunch of well known words
    c. Vertical: guessing passwords on the same account until successful
    d. Credential Stuffing: using passwords leaked from another site to test on accounts of the same login on different sites
11. Controls
    a. Directive: telling people what to do, AUP
    b. Detective: finding what people do, Log Reviews
    c. Corrective: Help in remedying a situation
    d. Deterrent Controls: discourage violations of security policy

   e. Preventative: teaching people what to do, Sec Awareness
   f. Compensating: helping mitigate human errors, MFA

12. A piece of hardware within a system that can always be trusted is a
    a. ROOT OF TRUST (RoT)
13. You need to ensure that data transferring between two long distance offices are secure. You will use:
    a. CELLULAR DATA
    b. WEP is old and out of data
    c. Bluetooth is too short distance
    d. Satellite is not consistent and very expensive
14. Corporate Cost Terms
    a. TCO - potential financial impact of a tool
    b. CAPEX - Capital expenditure; initial cost of something
    c. Operational Efficiency: effectiveness of operations
    d. ROI - Return on investment
15. Shadow IT vs Insider Threat
    a. Shadow IT uses banned apps for testing and innovation
    b. Insider Threats use banned apps for malicious intent
16. Fail Access Control Modes
    a. Fail-Closed: No Request allowed from unauthorized personell
    b. Fail-Open: All requests allowed
    c. Rate-Based Filtering: limits traffic based on a predefined rate
    d. Passive Mode: lets everyone in and passively monitors
17. CVE (Common Vulnerabilities and Exploits)
    a. A set of known vulnerabilities and exploits collected
    b. CVE Identifier Format: “2024-56789” - year, number
18. You are a cybersecurity analyst that collaborates with external companies. To ensure seamless login process between federations, the company should use:
    a. SAML to exchange ID information among organizations
19. To create a non-sensitive version of a data base is called:
    a. TOKENIZATION
20. Risk For Companies: Know the difference
    a. Risk Appetite: How much risk are we OK with?
    b. Risk Tolerance: How much risk can our company withstand
    c. Risk Acceptance: We can take the impact of this risk.
21. If an attacker is not inserting code but just moving around in a file system, it is…
    a. Directory Traversal
22. Certificates
    a. Self Signed Certificates - its in the name

    b. CSR (Certificate Signing Request) - formal message sent to a certificate authority to request digital identity certificate. Not a certificate by itself
    c. Wildcard Cert - used to secure multiple subdomains under a single domain
    d. Third-part certificate - signed and verified by an external certificate authority. Used by public and external environment due to inherent trust

23. If a WELL PAID insider believes that a government is CORRUPT and decides to take files for personal reasons to give to an enemy, that is POLITICAL, not espionage
24. Inputs are the required information for a process and the implications of their timing, NOT human and support resources
25. Probability
    a. The expected frequency of occurrence of a specific risk within a given time frame
26. LikelyHood
    a. Change of a risk occurring, low, medium, high
27. Exposure Factor
    a. Measures the likely hood of a vulnerability being exploited
    b. Unrelated to monetary losses
28. ARO (Annualized rate of occurrence)
    a. How many times a risk occurs per year
29. Key Escrow
    a. The process of giving a copy of a cryptographic key to a third party in case they are lost
30. Difference between Least Privilege and ACLs
    a. Least privilege can be applied to individual users while ACLs are criteria based
31. Penetration Testing Levels of approach
    a. KNOWN - user names and passwords
    b. Partically Known - general target systems known
    c. Unknown - no information given
32. Homomorphic Encryption
    a. Data-in-use can still maintain encryption while its being used
33. Remember that owners have ultimate decision making over data, whereas controllers determine the purpose and conditions of data processing in compliance with legal
34. File Metadata does NOT include the file extension
35. The more microservices, the more GRANULAR access control requirements
36. Record Level encryption is when you encrypt each file within a database
37. SASE (Secure Access Service Edge)
    a. Combines network security and WAN capabilities in a single cloud-based service, making it an ideal solution for ensuring secure and reliable access to data and applications irrespective of user/device location
38. Resource Reuse

    a. Vulnerability that involves accessing or modifying data or communications from other virtual machines by exploiting the shared CPU between them

39. CPU Starvation
    a. A process or thread does not receive enough CPU time to perform its tasks
40. TOC (Time Of Check)
    a. Type of race condition that occurs when a process checks the state of value of a resource before using it, but another process changes it in between.
41. Race Condition
    a. A situation where the outcome of a process depends on the timing or order of execution of other processes
42. The keylength in encryption standard is the MINIMUM amount of key length
43. KNOW ENCRYPTION!!!
    a. DES is for data
    b. SHA-256 is for passwords
    c. Twofish is for data
    d. ECC is for public key cryptography
44. Government Regulations
    a. Computer Security Act (1987) - requires federal agencies to develop policies to secure computer sustems that process sensitive or confidential information
    b. GDPR - EU regulation that protects personal data, NOT U.S.
    c. GLBA - focused on financial institutions; requires them to ensure security and confidentiality of customer data
    d. SOX - emphasizes transparency and accountability in financial reporting
45. E-Discovery
    a. Relates to the collection of electronic data - emails, databases, presentation files, voicemails, video/audio files, social media posts, and more.
46. Business Agreements
    a. SLA - outlines specific performance metrics, service levels, and responsibilities for ongoing services, but does not provide instructions or requirements for specific tasks or projects like SDE
    b. SOW (statement of work) - detailed instructions and requirements for tasks that will be carried out by a vendor, generally in a SDE project
    c. MSA - establishes long term partnership between an org and a vendor
    d. GPA - establishes an agreement between two orgs
47. Outtage Recovery
    a. MTTR - measured time to repair
    b. RPO - Recovery point objective - maximum allowable amount of data (measured in terms of time) that an organization can afford to lose during a disaster or an incident

    c. RTO - Recovery time objective - sets time goal to recover business processes after an outage
    d. BCP - business continuity planning - overarching process that includes recovery time objective, NOT time specific

48. CICD
    a. SPEEDS UP the development process, not slow down
49. Forcing users to create complex passwords is NOT GOOD PRACTICE
    a. Instead, have them create strong, unique passwords that they can remember for each account
50. Security Zones
    a. Segregate a network into different areas to control and restrict access based on business needs
51. UPS (uninterruptable Power supply)
    a. Provides IMMEDIATE, short term power when there is failure
52. Generator
    a. Provides long term power after starting up
53. Ticket creation is for COHESION
54. Encryption does NOT keep the structure of data intact
55. Masking DOES keep the structure of data intact. It is also confidential because it conceals original data with modified content.
56. The GDPR is for the entirety of the European Union, which is INTERNATIONAL
57. Agreements
    a. SOW (statement of work) - document with detailed instructions and requirements for a specific task within a project
    b. MSA (master service agreement) - comprehensive document that establishes the overall framework for a long-term business relationship between companies
    c. MOU (memorandum of understanding) - outlines that terms of a partnership between two organizations and how they will collaborate on specific projects. INFORMAL AGREEMENT MOU
    d. BPA (Business partner agreement) sets up a long term partnership between two companies. Does not focuson a specific work project.
58. Security updates are the BEST way to ensure known vulnerabilities are patched
59. Availability is the most important factor when considering different architectures.
60. Security key devices
    a. Secure Enclave - embedded into android and apple phones
    b. TPM - embedded into PC Motherboards
    c. HSM - physical computing device for storing digital keys
    d. KMS - a software for managing keys
61. 4 Stage Process of Vendors

a. Vendor Selection: pick a vendor that aligns with your company values and offers the right services
b. Master Service Agreement (MSA) - establish a framework for future business ventures
c. Vendor Monitoring: making sure that vendors continue to provide the right services with the right quality agreed upon
d. Vendor Assessment - Making sure that vendors are abiding by security regulations

62. Religious believers are protected under GDPR
63. Sanitation in asset management
    a. Erases all data from a storage device, rendering it unrecoverable
64. Race Conditions
    a. A bug that occurs when two processes or threads try to access and modify the same data at the same time without coordination
65. RC Exploits
    a. Time of Use - occurs when a process performans an action on a resource without verifying that it is still in the same state or value as when it was last checked.
    b. Time of Check - occurs when a process checks the state or value of a resource, but it changes in between.
66. Segmentation vs Isolation
    a. Segmentation divides a system into smaller, manageable parts to enhance performance and security
67. Passkey
    a. Asking a user to unlock his phone instead of requiring a password for every site.
68. Host-Bast Firewall vs Network-Based Firewall
    a. Host-based firewalls protect individual computers or servers by managing traffic directly on those hosts, while network-based firewalls secure entire networks by monitoring and controlling all traffic that passes through a designated gateway or network perimeter.
69. Rijndael
    a. The winner of the US Sponsored competition to be the new AES.
70. Understand Agent vs Agentless
    a. Agentless allows for actions to be initiated from servers, rather than individual user devices
    b. Agent-based means installing security monitoring programs on each user device for security monitoring
71. Quick Tip
    a. Read everything: if the question asks about viruses, understand what platforms are most susceptible to viruses.
    b. EMAILS are most susceptible.
72. Preventative vs Detterant Controls

    a. Preventative are unknown to malicious actors
    b. Deterrent are known and dissuade malicious actors mindfully.
73. Syslog
    a. A server on Unix and Linux platforms that stores system logs
74. ACL
    a. Can sit on network devices and filter traffic
75. SCADA (Supervisory Control and Data Acquisition)
    a. systems that are used to control and manage heating, ventilation, air conditioning, and other types of industrial and environmental systems.
76. Quick Tip
    a. Read and interpret everything. If the question asks, “For Security Reasons”, there must be a reason why it is specifying that.
77. DNS (Domain Name System) plays a crucial role in helping to verify the origin of email senders, primarily through mechanisms like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). These technologies are used to prevent email spoofing and to ensure that emails are not altered in transit, enhancing email security and sender verification.
78. DKIM (DomainKeys Identified Mail)
    a. Allows senders to associate a domain name with an email, vouching for its authenticity using a cryptographic signature.
79. SPF (Sender Policy Framework)
    a. Specifies which mail servers are permitted to send email for a domain
80. DMARC (Domain-Based Message Authentication, Reporting, and Conformance)
    a. Builds on DKIM and SPF. Allows for domain owners to specify policies on how to handle mail that doesnt authenticate with SPF or DKIM.
81. MTA (Mail Transfer Agent)
    a. Responsible for transferring an routing emails between servers, but doesnt employ crtographics signatures for sender authenticity.
82. Jump Server vs Forward Proxy Server
    a. Jump Servers act as an audit point and masks a destination IP
    b. Forward Proxy Servers act as a phonebook that direct traffic.
83. Containerization vs Segmentation
    a. Segmentation separates network and data layers. LOGICAL SEPERATION
    b. Containerization isolates application deployment and management. In the case of a multiple-use phone, it can separate personal info from business information
84. Recon vs Scanning
    a. Recon is often passive and comes before the intensive scans
85. Types of Cloud Providers
    a. Public - Third party that leases cloud to the public.

86. Spraying
    a. Using the same password on a bunch of user accounts
87. DDOS is a Spoofing attack as it masks IPs as it spams with requests
88. RADIUS is TCP port 1812
89. The Initiatlization Vector in the beginning of connections is the randomization element
90. OSI Model
    a. All People Seem to Need Data Processing
    b. 7 -> 1
    c. Upper level layers ca access the ones below it
91. Understand Classification
    a. Legal - legal data and regulatory compliance data
    b. Secret - Classification for the military
    c. Private - for corporations, may cause harm
    d. Confidential - Will cause serious harm
92. MITM Attacks
    a. Pass the Hash
        i. Attacker captures a hash used to authenticate a process
    b. Refactoring
        i. Attacker change the code without changing the function
    c. Replay Attacks
        i. Attacker may record packets send between a client and server during a valid login session and replay those packets at a later time
    d. Shimming
        i. Adding code between a driver and the OS.
93. Data Masking
    a. Technique of creating a mirror version of a database on which data modiciation techniques such as character shuffling, encryption, and wod or character substitution are applied to change the data
94. VLANs and Subnets
    a. You can use VLANs to correspond with subnets, separating groups of employees, data, teams, etc. logically.
    b. VIRTUAL, so no physical segmentation
95. When you get hacked or download malware,
    a. FIRST THING YOU DO IS GET OFF INTERNET AND TURN OFF DEVICE
    b. Then you contact Security Officers
96. Asking for strange information may indicate a phishing attempt
97. The incident response team should notified as soon as a incident response process is initiated, not in the prep phase.
98. There is no settings to prevent USB data transfer or charging. You must block both at the time time on all Operating systems.

99. Staging
    a. Testing and finalizing software in a controlled environment that simulates the production settings as closely as possible
100. Provisioning is about setting sup and preparing the infrastructure and resources needed for an application or service
101. Again, understand wording. If a question says, the cost associated with a single loss, think about SLE, single loss expectancy. The best description of impact is the damage that results from unmitigated risk.
102. Data in the EU is subject to its laws. Some data will also be required to be maintained on systems within the borders too
103. Malware and Viruses can come in the form of TCP traffic, so firewalls wont prevent it.

Security Architecture

- Cloud Architecture
    - IaaS (Infrastructure)
        - Think about computing resources
    - PaaS (Platform)
        - Think about testing environments
        - Subnets, networking, VLANs are already created for you
    - SaaS (Software)
        - Applications are provided on demand
- IaC (Infrastructure as Code)
    - A methodology that creates repeatable processes for deploying infrastructure
    - Replaces static scripts (used once and thrown away)
- CI/CD Pipeline
    - The process of developing, testing, fixing continuously throughout a development process.
- Serverless Computing
    - Someone else manages the servers
    - User just focuses on their own development
- Microservices
    - Collection of loose coupled independently deployable services
        - Each can be deployed, patched, updated, and scaled
        - Faster development bc nothing is connected
- Software Defined Networking
    - Decoupled the management plane from the data plane
    - Places intelligence high up the stack
    - Programmatic tuning based on activity, workloads, etc.
- SCADA Systems

    - Centralized Aggregated System with a bunch of screens used to operate industrial systems
    - Used to be monolithic closed systems, now is more open and connected to IoT Devices, Networking, and Internet
- Understand these working formats
    - Remote: Each individual worker is at home
    - Decentralized: Groups or teams are working and distributed to various company locations
    - Centralized: One big office
- Inline/Active vs Monitoring/Passive
    - Inline includes IPS and Firewalls that monitor, alert, and take action
    - Monitoring includes IDS and anything else that scans and does nothing else.
- Audit trails vs Incident Logs
    - Audit trails are detailed records that log sequential activities within a system
    - This is useful to aid in the detection and examination of security breaches
- Next-Generation Firewall
    - Provides advanced integrated security features like intrusion prevention and user identity tracking
- SD-WAN
    - Faster speeds at lower costs to connect enterprise networks over large geographic distances
- Operational vs Technical Security Controls
    - Operational is reviews and monitoring of event logs and such
    - Technical is firewall, IDS/IPS, encryption, access controls
- Understand Legacy vs End-of-Life
    - Legacy hardware could still be supported by a manufacturer, it just might be built on older architecture, leading to possible unfixable vulnerabilities
    - End-Of-Life hardware means that while a piece of equipment could still be modern, it is no longer supported software-wise by its manufacturer

Other Tips

- When it comes to testing a newly integrated piece of equipment, penetration testing is the best way to ensure that no potential security gaps exist
- Read everything, dont skip to the end and look for “security”. There might be phrases like, “in terms of compute considerations” in which youll have to pick the answer “resource allocation and scalability” instead of a answer that would be correct if it wasnt there
- Never completely block USB ports or email attachments. It will disrupt business operations. Just scan and protect what is being sent over.