CompTIA Security+ SYO-701 Professor Messer Course Notes

Study online at https://quizlet.com/_evqwjz

1.	**Security Control Categories (List All 4)**	Technical, Managerial/Administrative, Operational, Physical
2.	**Security Control Types (List All 6)**	Preventive, Deterrent, Detective, Corrective, Compensating, Directive
3.	**CIA Triad**	Confidentiality, Integrity, Availability
4.	**AAA Framework**	Authentication, Authorization, Accounting
5.	**Gap Analysis**	Analyzing the gap between the current security posture and the goal security posture of the organization
6.	**Zero Trust**	A wholistic system that covers every device, process, and person, requiring verification for everything, nothing is inherently trusted
7.	**Planes of Operation (List Both)**	Data Plane and Control Plane
8.	**Policy Decision Point (PDP)**	Entity which receives untrusted requests, made up of a Policy Engine and Policy Administrator
9.	**Policy Engine**	Evaluates access decision based on policy and other information, grants, denies, or revokes access
10.	**Policy Administrator**	Generates Access Tokens or credentials, Communicates with the Policy Enforcement Point (PEP)
11.	**Policy Enforcement Point (PEP)**	Endpoint which receives untrusted requests and sends them to the PDP
12.	**Access Control Vestibule**	A room that controls the movement of people who go through it, usually at the entrance to a building

13.	**Honeypot, Honeynet, Honeyfile, Honeytoken**	A Fake network, system, token, etc to attract and trap threat actors
14.	**Key Escrow**	Someone else holds your private keys
15.	**Key Stretching**	Make a weak key stronger by performing multiple processes with the same key, encrypting multiple times, hashing multiple times etc.
16.	**Out-Of-Band Key Exchange**	Transfer an encryption key OFF of the internet, over the phone, in person, etc
17.	**In-Band Key Exchange**	Exchanging encryption keys over the network, using encryption or something else
18.	**Trusted Platform Module (TPM)**	Device that contains cryptographic hardware, includes key backup, cryptographic accelerators, etc/
19.	**Secret Enclave**	Protected area for encryption secrets
20.	**Attributes of Threat Actors (List 4)**	Internal/External, Level of Sophistication/Capability, Resources, Motivation
21.	**Watering Hole Attack**	Infect a 3rd party site, network, tool, etc with malware and wait for target to arrive
22.	**Memory Injection**	Malware injects itself into the memory of an already running process
23.	**DLL Injection**	Malware injects a path to a malicious DLL (Dynamic Link Library) Into existing windows process, one form of Memory Injection
24.	**Buffer Overflows**	Overwriting a buffer of memory to change something in another separate memory area

25.	**XSS (Cross-Site Scripting) Attack**	An attack where a threat actor injects code into a website to make a request to a third party using that user's authentication information
26.	**Directory Traversal**	Allows applications to access data outside of their own folder using ../../..
27.	**Worm**	Malware that self-replicates through the network, not requiring human interaction
28.	**Rootkit**	Malware that modifies core system files, invisible to the operating system
29.	**Environmental Attack**	Attack everything supporting the technology, the power, HVAC,
30.	**DNS Poisoning**	Modify a DNS server to route a URL to a malicious IP address
31.	**Domain Hijacking**	Get access to a domain registration, move traffic flow towards malicious sites
32.	**Birthday Attack**	An attack that takes advantage of hash collision
33.	**Spraying Attack**	Try 3 most common passwords on a ton of different accounts so you don't get locked out
34.	**Out-Of-Cycle Logging**	Logs coming in at an unexpected time, an indicator of compromise
35.	**ACLs (Access Control Lists)**	List to allow or disallow traffic, from source and destination IP, port number, time of day, application, etc
36.	**SSH Port**	22 TCP
37.	**HTTPS Port**	443 TCP
38.	**HTTP Port**	80 TCP
39.		

	EDR (Endpoint Detection and Response)	System that detects threats on endpoints throughout a network
40.	**SCADA / ICS**	Supervisory Control and Data Acquisition System , a large scale, multi-site Industrial Control System, usually air-gapped and controls industrial equipment
41.	**RTOS (Real-Time Operating System)**	An operating system with a deterministic processing schedule, meaning that each process is guaranteed to be executed in a specific amount of time, without waiting for other processes.
42.	**Availability Vs Redundancy**	Available means constantly up, if something is redundant but not available it might require manually turning on the replacement infrastructure
43.	**Security Zones**	Zone-based security technologies, labeling certain parts of the network as trusted, untrusted, screened, etc.
44.	**Fail Modes (List 2)**	Fail-Open, meaning when the system fails, data continues to flow, Fail-Closed, when the system fails, data does not flow
45.	**IPS (Intrusion Prevention System)**	System that watches network traffic looking for intrusions, both preventing and detecting
46.	**Forward Proxy**	Also known as an internal proxy, exists inside the network
47.	**Reverse Proxy**	Direct inbound traffic from the internet to the proxy on your network
48.	**Open Proxy**	Third Party, Uncontrolled proxy out on the internet
49.	**IEEE 802.1X**	Port-based network access control, you don't get access to the network until you authenticate
50.	**EAP**	

		Extensible Authentication Protocol, provides many different ways to authenticate, integrates with 802.1X
51.	**Traditional vs NGFW Firewall**	Traditional firewall can't filter on application information, only port numbers, Next-Gen can also do content filtering, control website traffic by category, and serve as IPS systems
52.	**UTM (All-in-one Security Appli-cance)**	Firewall that can also do a ton of other stuff, filter spam, inspect for malware, serve as a router, a switch, and an IPS/IDS system
53.	**WAF (Web Appli-cation Firewall)**	A firewall that runs in the browser
54.	**SD-WAN**	Software Defined Networking in a Wide Area Network a WAN built for cloud services so cloud applications can communicate directly without hopping through a central point
55.	**Data Sovereignty**	Data that resides in a certain country is subject to the laws of that country
56.	**Data Masking**	Hide some of the original data, like ******123 with credit card numbers
57.	**COOP (Continu-ity of Operations Planning)**	A plan for continuing the organizations operations if all the technology is disabled
58.	**Fail Over**	Plan for the worst case scenario to keep running with alternate infrastructure to "fail over" to
59.	**Recovery Test-ing**	Simulating a situation where data is lost and we restore to a backup
60.	**Replication**	An ongoing real-time backup, keep data synchronized in multiple locations

61.	**Journaling**	Writing data to storage in chunks, make a journal entry when start writing, close it when done, so that if the system goes down while writing you can distinguish corrupted data
62.	**UPS (List 3 Types)**	Uninterruptible power supply. Offline/Standby, Line-Interactive, On-Line/Double Conversion
63.	**Site Surveys**	Sample existing wireless landscape in a location
64.	**MDM**	Mobile Device Management, centralized management of mobile devices
65.	**BYOD**	Bring Your Own Device, technology or devices that employees bring in, need to meet the company's requirements
66.	**COPE**	Company Owned, Personally Enabled, a device that the company buys, but can also be used as a personal device
67.	**CYOD**	Choose your own Device, similar to COPE, but the user gets to choose the device
68.	**WPA2 vs WPA3**	WPA2 has a vulnerability that allows the PSK to be brute forced or captured over the network, WPA2 solves this problem
69.	**SAE**	Simulataneous Authentication of Equals, a Diffie-Hellman derived key exchange with an authenticatino component, everyone uses a different session key, even with the same PSK, an IEEE standard, the Dragonfly Handshake
70.	**RADIUS**	Remote Authentication Dial-In User Service One of the more common AAA protocols, centralize authentication for users
71.		

	Static Code Analyzer (SAST)	Static Application Security Testing analyzes code to help identify security flaws, has false positives
72.	**Fuzzing (Dynamic Analysis)**	Input randomized input to applications to find vulnerabilities
73.	**CTA**	Cyber Threat Alliance, an alliance of organizations which share information about cybersecurity threats
74.	**OSINT**	Open Source Intelligence, contains a collection of known threats
75.	**Responsible Disclosure Program**	controlled release of information about vulnerabilities, bug bounties
76.	**CVSS**	Common vulnerability Scoring system, quantitative scoring of a vulnerability used in the National Vulnerability Database
77.	**SIEM**	Security information and event Manager, an application that colocates security logs from across the network into one place
78.	**DLP**	Data Loss Prevention
79.	**SNMP**	Simple Network Management Protocol, polls devices for statistics at fixed intervals, can be set up for alerts called SNMP traps
80.	**Active Directory**	a database of everything on the network, primarily windows based
81.	**FTP Port**	20, TCP
82.	**Telnet Port**	23
83.	**IMAP Port**	143 TCP
84.	**SPF**	Sender Policy Framework, sender configures a list of all servers authorized to send emails for a domain

85.	**DKIM (Domain Keys Identified Mail)**	A Mail server digitally signs all outgoing mail, the signature is validated by the receiving mail servers
86.	**DMARC**	Domain-Based Message Authentication, Reporting and Conformance an extension of SPF and DKIM, the domain owner decides what receiving email sdervers should do with emails not validating using SPF and DKIM, accept all, send to spam, or reject, creates compliance reports sent to email administrator
87.	**FIM (File Integrity Monitoring)**	monitor important files that should never change with hashes, in windows its SFC in linux its tripwire
88.	**Extended Detection and Response (XDR)**	An evolution of EDR improves missed detections, false positives, etc. Adds network-based detection
89.	**IAM**	Identity and Access Management, manages identities and authorization for different resources
90.	**LDAP (Lightweight Directory Access Protocol)**	Protocol for reading and writing directories over an IP network
91.	**Security Assertion Markup Language (SAML)**	Open standard for authentication and authorization
92.	**Access Control Types (List 5)**	Mandatory (Based on levels of security clearance, confidential, secret, top secret, etc) Discretionary (Based on data ownership, the creator of data decides who has access to it) Role-Based access Control (Different roles in the org have different levels of access) Rule-Based Access control (generic system enforced

		rules for access) Attribute-Based (Complex relationships between users and data, may be based on many different criteria)
93.	**MFA types (List 4)**	Something you know Something you have Something you are Somewhere you are
94.	**NIST SP800-61**	National Institute of Standards and Technology, computer security incident handling guide
95.	**Incident Response Lifecycle**	Preparation Detection & Analysis Containment, Eradication, & Recovery Post-Incident Activity
96.	**Acceptable Use Policies (AUP)**	Detailed documentation on the acceptable use of company assets, internet, telephone, etc.
97.	**ARO (Annualized Rate of Occurence)**	how likely is it that a certain disaster will happen over the course of a year
98.	**Exposure Factor (EF)**	the percentage of the value that is lost due to an incident, from 0-1.0
99.	**SLE (Single Loss Expectancy)**	What is the monetary loss if a single event occurs? Exposure Factor x Asset Value
100.	**ALE (Annualized Loss Expectancy)**	Annualized Rate of Occurence * Single Loss Expectancy

101. **Risk Appetite vs Tolerance**	Appetite is the acceptable amount of risk, tolerance is the tolerable amount of risk, which is higher
102. **DKIM**	Domain Keys Identified Mail A mail server digitally signs all outgoing mail, the receiving mail server validates the signatures
103. **MTTR**	Mean Time To Repair Average time required to fix a failed system, including the time for diagnosing the issue
104. **MTBF**	Mean Time Between Failures total uptime/number of breakdowns average amount of time between failures
105. **RTO**	Recovery Time Objective Amount of time that the organization can tolerate for system recovery, once the database and server are operational
106. **RPO**	Recovery Point Objective The acceptable amount of data loss in the case of an outage
107. **SLA**	Service Level Agreement Minimum terms for services provided, uptime, response time agreement, etc. Commonly used between customers and service providers
108. **MOU**	Memorandum of Understanding Both sides agree in general to the contents of the memorandum, usually states common goals, but not much more, may include statements of confidentiality, informal letter of intent; not a signed contract
109. **MOA**	Memorandum of Agreement The next step above a MOU, Both sides conditionally agree to the objectives, can also be a legal document, even without legal language, unlike a contract, may not

	contain legally enforceable promises
110. **MSA**	Master Service Agreement, Legal contract and agreement of terms, a broad framework to cover later transactions. Many detailed negotiations happen here, future projects will be based on this agreement
111. **WO/SOW**	Work Order / Statement of Work Specific list of items to be completed, requires an MSA, details all of the legal requirements for a job, referred to to determine completion
112. **BPA**	Business Partners Agreement Agreement for two businesses going into business together, lists out who makes business decisions and scope, contingency and disaster recovery plans
113. **Data Custodian**	The role responsible for handling data accuracy, privacy and security
114. **Data Controller**	Manages the purposes and means by which personal data is processed
115. **Data Processor**	Processes data on behalf of the data controller, often a third-party or different group
116. **Data Owner**	Usually a higher up who owns the data
117. **CRL**	Certificate Revocation List
118. **OSINT**	Open Source Intelligence sources, gathering information from publicly available data, social media, etc.
119. **Active Recon**	Gathering information while interacting with the subject directly, in a way that usually can be discovered, pings, dns queries, requests, etc.
120. **Passive Recon**	

		Gathering information on a subject without interacting with them directly, in a way that can't be discovered, through social media, the web site, etc.
121.	**Shadow IT**	Groups or individuals within IT departments who work without the company's knowledge, going rogue, building their own infrastructure in the cloud
122.	**Risk Transfer**	Transfer the risk to another party, like buying cybersecurity insurance.
123.	**Risk Acceptance**	Taking on the risk yourself
124.	**Exception vs Exemption**	Exemption is if a security policy cannot be followed, Exception is when a security policy isn't applied for a temporary period
125.	**Risk Avoidance**	Stop participating in the high risk activity itself
126.	**Risk Mitigation**	Reducing the impact of a risk event by reducing the probability of its occurrence
127.	**IP-sec**	Site-To-Site VPN encrypted transfer tunnel protocol
128.	**MSP**	Managed Service Provider
129.	**Attestation**	Provides an opinion of truth or accuracy of a company's security positioning, An auditor will attest to a company's cybersecurity posture
130.	**Self-Assessment**	The organization performs it's own checks
131.	**CSR**	Certificate Signing Request, a CA validates the request, and digitally signs the certificate
132.	**OCSP**	Online Certificate Status Protocol, an alternative to CRL, allows certificate holders to verify the status of their own certificates, revoke or validate, etc.
133.	**TPM**	

	Trusted Platform Module, a hardware chip on the motherboard that includes a bunch of cryptography technology, random number generator, persistent storage for keeping burned in keys, and password protected
134. **HSM**	Hardware Security Module, a network appliance used for larger environments than a TPM, much more high end cryptographic technology
135. **Secure enclave**	Protected area for secrets, usually implemented as a hardware processor thats isolated from the core processor, has a real random number generator, has its own boot rom, monitors the boot process
136. **Rogue Access Point**	A rogue access point is an unauthorized access point added by a user or attacker. This access point may not necessarily be malicious, but it does create significant security concerns and unauthorized access to the corporate network.
137. **Obfuscation**	The process of making something unclear, hiding data in plain sight, steganography