1.What are the three kind of assets we need to protect? Hardware, Software, Data
2.Which asset is the most valuable? Data - Not easily replaceable
3.How can timing impact the value of an asset? It may cause other times of harm
4.Define the following:
   a. Vulnerability -Weakness in a system
   b. Harm - Negative consequence of an attack
   c. Threat - Potential to cause harm
   d. Attack - attempt to compromise vulnerability
   e. Control - An action or procedure that reduces vulnerability
5. What is security triad?
   a. Confidentiality - Property that is only viewed by authorized parties
   b. Integrity - assets only modified by authorized party
   c. Availability - assets used by authorized party at authorized time
6. What are the three extra properties that complement the security triad?
   a. Authentication - Confirm Identity of center of information
   b. Non-repudiation - Confirm that sender of data cannot deny it
   c. Auditability - Ability to trace previous history
7. What are 4 general types of computer attacks?
   a. Interruption
   b. Interception
   c. Modification
   d. Fabrication
8. Give examples of non-human threats
   a. Natural Disaster
   b. Loss of Power
   c. Malfunction of hardware
9. What is an advanced persistent threat? A name of class of attack that's based on timing
10. Do we need to be concerned with non malicious human threats? Yes. Typos, spilled drinks, deletion
11. What is the difference between a random and directed threat? Directed attacks are targeted to a particular party whereas random could be anyone. Ie phishing website.
12. What is the CVE list? Common Vulnerabilities & Exposures
13. What is CVSS? Common vulnerability scoring system
14. What are the four categories of types of attackers?
   a. No Pattern
   b. Individuals
   c. Organized world groups
   d. Organized Crime, terrorists
15. What are examples of types of harm that can occur?
   a. Financial
   b. Reputation
   c. Time
   d. social/emotional

    e. Physical harm
16. Name and define/describe three components of MOM
    a. Method - ability, skill level, tools
    b. Opportunity - not an issue, capable of doing it
    c. Motive - notoriety, political, money,fame, challenge, revenge, just because
17. How important is MOM in cybercrime as compared to regular physical crimes like burglary? MOM is significantly more important as issues can scale to millions of people. Cause more harm
18. What is the attack surface? Full set of vulnerabilities
19. What are the 6 ways to deal with harm?
    a. Prevent - block attack or remove vulnerabilities
    b. Deter - make attack harder
    c. Deflect - make another target look more attractive
    d. Mitigate - make successful attacks less severe
    e. Detect - Identify that something happened
    f. Recover - restore to proper state
20. What are the three categories of physical controls?
    a. Hardware
    b. Software
    c. Configurations
21. What does a security policy have to do with being able to tell if a company is “secure”? The security policy has to meet its requirements of what is defined to be secure.
22. What is authentication? Proving you are who you say you are
23. What is identification? Act of asserting who a person is
24. What are the three general categories of methods to perform authentication?
    a. Know - known password
    b. Are - biological fingerprint, face recognition
    c. Have - Key, phone
25. Name issues/problems associated with using passwords?
    a. Hard to remember
    b. Generally not Secure
    c. Can be duplicated
    d. Revocation
26. What’s the difference between a brute force attack and a dictionary attack? Brute force is all possible combinations whereas dictionary tries common words with various permutations.
27. What are some examples of likely passwords
    a. Generally - family names, birthdays, pet names
    b. Specifically - home town and street they grew up on, places, etc
28. How should passwords be stored? In a hash with an added salt
29. What is a rainbow table? A table of hashes used for reversing cryptographic functions to hack into systems
30. What prevents identical passwords from looking identical when stored? A salt
31. What are some methods for creating good passwords? Create variant of PW’s. Random substitution. Mnemonic passwords

32. What are problems/issues with biometrics? They are non revocable, slow, intrusive, can give false readings, expensive, and no backup method.
33. What types of false readings can biometrics have? What is the potential impact of those false readings? True pos, false pos, false neg, and true neg. This can lead to someone not being able to access information they are authorized for or being able to access information they are not authorized for.
34. Are biometrics good at identification or authentication? They're okay at identification but best at authentication. Too slow for identification in large systems.
35. What is the most common example of "Something you have" that is used for authentication? Your phone.
36. What is the difference between an active and passive token?
    a. Active - Communicates with sensor
    b. Passive - Does not interact
37. What is the difference between a static and dynamic token?
    a. Static - Values don't change. Ex cookies
    b. Dynamic - Values Change. Ex Duo
38. What is multifactor authentication? Using multiple methods to authenticate user
39. What is federated id management, and how is it closely related to single sign on? Federated ID management uses central authentication. (Auth Server) that logs you into every other service as well. SSO uses one auth server but you must log in separately to separate services.
40. What is cryptography? Secret writing/communication
41. What is cryptanalysis? Deciphering messages without being told the key
42. What is a cryptosystem? Entire system for encoding, decoding
43. What is security by obscurity as it relates to cryptography? Relying on secrecy as main method of protection
44. Should encryption algorithms be kept secret? No, because if they were private there could be back doors, people could hack, etc. Public ensures there are no backdoors and the algorithms are strong.
45. Should encryption keys be kept secret? Yes. This is what protects your encoded message. It's a private key.
46. What does work factor mean, as it relates to crypanalysis? How long it would take to crack. 25 char, lowercase, instructions per second, etc.
47. What is symmetric key encryption? A type of encryption that uses the same key to encrypt and decrypt messages.
48. What are some properties of symmetric key encryption? Very fast. Subject to man in the middle attacks
49. Compare stream and block ciphers.
    a. Stream - letter by letter. Very small chunks. Computationally expensive. Low diffusion
    b. Block - group by group. CPU inexpensive. High diffusion
50. What is confusion/substitution? They work to thwart application of statistics and other methods of cryptanalysis
51. What is diffusion/transposition? Using statistics and other means to rearrange the information

52. What is DES, and what are important properties? 1970's IBM. 56 bit encryption. 8 bits unused data, encrypts 64 at a time.
53. What was the original name for DES? Digital Encryption Standard
54. What is 2DES, and what are important properties? Double DES. E(k2,E(K1,P)) 112bit key, 57 bit strength
55. What is 3DES, and what are important properties? Triple DES = standard. E(K1,E(K2,E(K3,P))) 168 bit key length = 112 bit strength.
56. What does the NSA have to do with DES? THey made changes to Lucifer and never explained why.
57. What is AES?. Netherlands peopole 1997 public competition. Supports many encryption sizes
58. Advanced Encryption Standard
59. A private meeting with public people voicing opinions. From a competition
60. What are important properties of AES? 128,196,256, more. 128 block size. 10,12, or 14 cycles
61. Is key management a positive or negative feature of symmetric encryption? Negative. If you lose a key, the cryptography is compromised
62. What is Diffie Hellman, and what is it's major weakness? 1976 asymmetric key crypto. Public key. Discrete log problem. No Authentication, man in middle vulnerability
63. What are some important characteristics of RSA? Rivest Shamir Adelman 1978. 256 bit key minimum. Very Slow. Authenticates
64. In what way are asymmetric and symmetric encryption used together? Use asymmetric encryption to pass the symmetric key to establish a fact, secure connection
65. What property do you get in asymmetric encryption when you are able to decrypt properly with a private key? Authentication
66. What property do you get in asymmetric encryption when you are able to decrypt properly with a public key? Integrity
67. What are the names for a hash? Checksum, message digest. One way to encrypt, no way to decrypt.
68. Why is a hash not true cryptography/encryption? It's just a representation of the set of data.
69. What Is a collision? Two things hash to the same value
70. What are the two most commonly used hash algorithms? MD5 and SHA