1. These are raw facts with unknown coding schemes? **Noise**
2. These are accepted facts, principles, or rules of thumb that are useful for specific domains. This can be the result of inferences and implications produced from simple information facts: **Knowledge**
3. It is an assurance that the sender is provided with proof of data delivery and the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.: **non-repudiation**
4. These are security measures to establish the validity of a transmission, message, or originator.: **Authentication**
5. Enumerate the IA four security engineering domains: **physical security, personnel security, its security, operational security**
6. This refers to the protection of hardware, software, and data against physical threats to reduce or prevent disruptions to operations and services and loss of assets. **Physical Security**
7. What are three distinct levels protecting information that Information Assurance can be thought of? **Physical, perceptual, and information infrastructure**
8. What level of focus does information assurance covers information and data manipulation ability maintained in cyberspace, including data structures, processes, and programs, protocols, data content and databases? **information infrastructure**
9. According to studies, what is the biggest threat to computer security**? Malware**
10. What are the components of an information that makes it more significant compare from other type of data? Choose all that apply. **Perceptual, accurate, verifiable, comprehensive**
11. Which of the following statement best describe Hackers? **One who gains unauthorized access to or breaks into information systems for thrill, challenge, power or profit**
12. What category of security solution/policy is phrased in terms of entities that execute activities and request access to object? **Subjects**
13. Is a category of entities, or a circumstance, that poses a potential danger to an asset? **Threat**
14. What are the three categories of threat? Choose all that apply? **By impact, by intent, by kind of entity involve**
15. What term is used to describe a program written to take advantage of a known vulnerability? **Exploit**
16. A Vulnerability in Cisco IOS that allows attackers to gain control of the routers, monitor network communication, and infect other network devices. **Synful knock**
17. It is the manipulation of an individual into performing actions or divulging confidential information**: social engineering**
18. A type of password cracking where the attacker tries several possible passwords in an attempt to guess the password. **brute-force attack**
19. An infiltration method where a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source, tricking the recipient into installing malware on their device or sharing personal or financial information. **Phishing**
20. What algorithm calculates a string value from a file of a fixed size, that contains data, and transformed it into a short fixed key or value? **hashing**