**CSC 312 Cybersecurity**

|  |  |  |
| --- | --- | --- |
| **50 Points** |  | **Assignment 01** |

**Fill in the Blank (20 Points)**

1. Masquerade is an attack in which the attacker assumes the identity of another computer user
2. Vulnerability is a weakness in a boundary or other defense that could enable an attack
3. Subversion is an attack in which a program is modified to operate on behalf of the attacker
4. Hunter’s Dilemma is protecting oneself while leaving a neighbor vulnerable to attack
5. Least Privilege is the principle of granting the minimum permissions needed to get work done
6. Acceptable use policy (AUP) is a written set of rules for the use of certain assets, typically information assets
7. Confidentiality protects sensitive information from disclosure to unauthorized recipients
8. Black-hat is a hacker who uses knowledge of security weaknesses to attack computer systems
9. Continuous Improvement is a cyclical process that improves future performance based on past results
10. Risk Assessment is the security process phase in which we identify and prioritize threats
11. Defense is a security measure intended to resist an attack
12. Forgery is an attack using bogus information that appears legitimate
13. Compromised system is a system that is no longer safe to use because it has been attacked
14. Ransomware is an attack that prevents authorized users from using an information system
15. Ethical hacker is a hacker who uses knowledge of security weaknesses to protect computer systems
16. Active attack is an attack that either injects new information into the system it attacks or modifies information already there
17. Worm is malware that constantly scans the Internet for vulnerable computers
18. Botnet is a collection of networked computers remotely controlled by an attacker
19. Passive attack is an attack, which simply collects information without modifying the system it attacks
20. Malware is malicious software that exploits weaknesses in people's computers

**Multiple-choice questions: (8 points)**

1. CIA properties do *not* include:
2. confidentiality
3. integrity
4. authentication
5. availability
6. When you analyze a system using the six-phase security process, you are performing a:
7. risk assessment
8. boundary analysis
9. security architecture study
10. plan-do-check-act cycle
11. An attempt by a threat agent to exploit assets without permission is referred to as:
12. an attack
13. a vulnerability
14. a safeguard
15. a trade-off
16. A security analyst is performing a security assessment. The analyst should not:
17. get written authorization from the organization to verify that the assessment should take place
18. take actions to mitigate a serious risk
19. protect all working notes
20. securely erase all collected information that’s not needed for business purposes
21. When disclosing a security vulnerability in a system or software, the manufacturer should avoid:
22. patching the system or software
23. including enough detail to allow an attacker to exploit the vulnerability
24. notifying customers
25. all of the above
26. Car ignition Locks are an example of what type of decision:
27. Requirement Based
28. Relativistic Based
29. Rule Based
30. Hunter’s Dilemma
31. Anonymous is an example of what kind of agents.
32. Threat
33. Military
34. Intelligence
35. Secret
36. This yields a more specific set of attacks tied to our particular threat agents.
37. Threat Matrix
38. Security Matrix
39. \_\_\_\_\_\_\_
40. Attack Matrix

**True or False Questions (12 points):**

|  |  |  |
| --- | --- | --- |
| # | Statement | True or False |
| 1 | The term “security theater” refers to security measures intended to make potential victims feel safe and secure without regard to their effectiveness. | T |
| 2 | Authentication is a security service that ensures information is reliably available. | F |
| 3 | People can be threat agents in some cases but trustworthy in others. | T |
| 4 | A vulnerability is a security measure intended to protect an asset. | F |
| F | Botnets can (often) perform distributed denial of service (DDoS) attacks in which thousands of individual computers send overwhelming amounts of traffic at a victims computer. | T |
| 6 | In requirements based security, we identify and prioritize our security needs in a risk assessment process. | T |
| 7 | Security Category RMF begins with a high level estimate of the impact caused by cyber security failures. | T |
| 8 | A threat agent is a person who did attack our assets, an attacker might attack an asset. | F |
| 9 | Information security architecture often relies on boundaries outside the computer to protect important information or programs from error prone or malicious programs. | F |
| 10 | Once we have filled in the attack likelihoods and impacts we compute the significance by multiplying these values together. | T |
| 11 | To analyze a risk, we review it against the threat agents behind the risk. | T |
| 12 | Zero Day vulnerability is one that has been reported to the software’s vendor and the general public. | F |

**Essay Questions (10 points):**

1. List the 3 key concepts of IT Security

Confidentiality

Integrity

Availability

1. Identify the five general steps of a security risk assessment.

### 1. Determine the Scope of the Risk Assessment

### 2. Threat and Vulnerability Identification

### 3. Analyze Risks and Determine Potential Impact

### 4. Prioritize Risks

**5. Document All Risks**

1. You are performing a risk assessment and prioritizing risks. You have estimated the cost of a loss caused by a certain attack. You estimated the potential frequency of the event over a period of time, and multiplied the cost times the frequency (the cost over that time period). Identify two reasons why the results may be misleading.

-Threat Event Frequency and it’s accuracy would be hard to pin down which would directly affect the cost of loss.

-Asset cost may fluctuate overtime.

e.g.The first replacement vs the tenth replacement might be different