|  |  |  |
| --- | --- | --- |
| **CSC 312 Cybersecurity** | **Assignment 04** | **50 Points** |

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

1. Active token is an authentication device that produces a different credential each time it is used.
2. Credential is a block of data provided by a user for authentication purposes; may be a static or a changing value.
3. Dictionary Attack is a trial-and-error attack that uses a list of items (the dictionary) as the source of the trials it performs.
4. Multi-factor authentication is an authentication mechanism that relies on two of the three authentication factors.
5. Hash function is a function that produces a hard-to predict output of fixed size when provided a block of input data.
6. Passive token is an authentication token that always produces the same credential, e.g. a magnetic stripe card
7. Password cracking is an attack in which an attacker tries to guess passwords for a system, often through an off-line attack.
8. PIN (personal identification number) is a memorized number occasionally used in two-factor or three-factor authentication systems.
9. Search space is the set of all possible values that a piece of secret information (i.e. a password) may possibly have.
10. Social engineering is an attack in which the threat agent uses social pressure to induce people to unknowingly aid the attack.
11. One common OS security threat is password attacking which can be mitigated by choosing complex passwords and using different passwords for different accounts.
12. In network security, foot printingis the initial step where an attacker gathers information about the target to help make the attack successful.
13. Defensive cybersecurity focuses on protecting against cyber-attacks by using a variety of security measures during investigations and stopping attacks as they happen.
14. Digital forensics involves collecting and investigating digital evidence in the context of a cyber incident or crime.
15. A Security Operations Center (SOC) is responsible for continuously monitoring, detecting, analyzing and responding to any cybersecurity incidents on a company's network and systems 24/7.
16. In a SOC, one of the data sources is

network activity/security events

threat intelligence

endpoint activity

authorization

which can include mail server, web server, and domain controller logs.

1. A SOC often uses a SIEM system to aggregate data from different sources and efficiently correlate the data to respond to attacks.
2. In network security, the Delivery stage involves sending the malicious code to the target via any feasible method, such as email or a USB.
3. The principle of least privelege should be applied to address Weak File Permissions in operating system security.
4. In digital forensics, establishing a chain of custody is important to ensure only authorized investigators access the evidence and to prevent tampering.

**Multiple-choice questions: (10 points)**

1. The following are fundamental strategies for authenticating people on computer systems *except*:
2. something you know
3. something you have
4. something you are
5. something you make
6. An attack in which someone tries to trick a system administrator into divulging a password is called:
7. denial of service
8. social engineering
9. sniffing
10. trial and error
11. Authentication does what:
12. Associates an individual with an identity
13. Checks access rights
14. Grants access rights
15. All of the above
16. The following risks are associated with a weak threat except.
    1. Shoulder surfing
    2. Simple trial and error password guessing
    3. Searching for a written password
    4. All are risks associated with a weak threat
17. In a password system, increasing the work factor:
18. increases the length of the password
19. decreases the length of the password
20. increases the size of the character set from which users choose passwords
21. a and c
22. Which of the following is NOT part of the basic scope of Offensive Security?
23. Operating System Security
24. Web Application Security
25. Network Security
26. Digital Forensics
27. Which of the following is a common web application security threat?
28. Injection
29. Encryption
30. Secure file transfer
31. Strong password policies
32. In the context of network security, what does the term "recon" stand for?
33. Recovery
34. Record
35. Reconnaissance
36. Reconfiguration
37. In digital forensics, what is the primary purpose of creating a forensic copy of the evidence?
38. To manipulate the original data
39. To prevent altering the original data during analysis
40. To make the original data more accessible
41. To share the original data with multiple parties
42. What is the purpose of a Security Information and Event Management (SIEM) system in a Security Operations Center (SOC)?
43. To exploit vulnerabilities in computer systems
44. To aggregate and correlate data from different sources for efficient response to attacks
45. To store user passwords in plain text
46. To develop new hacking techniques**True or False Questions (10 points):**

|  |  |  |
| --- | --- | --- |
| # | Statement | True or False |
| 1 | After encrypting a plaintext file, it should actively erase the plaintext file's context and save the encryption. | T |
| 2 | Some challenge-response systems use a token as part of the user identification process. | T |
| 3 | When you are biased in selecting a password, you choose your password from the entire search space. | F |
| 4 | Biometric readers have a large allowance for error in reading and conditions of the body. | F |
| 5 | Tokens are favored over passwords as they are immune to sniffing and trial-and-error guessing. | T |
| 6 | Offensive cybersecurity focuses on protecting user data and stopping attacks as they happen. | F |
| 7 | A Security Operations Center (SOC) is primarily responsible for developing new hacking techniques. | F |
| 8 | SIEM systems are used in a SOC to exploit vulnerabilities in computer systems. | F |
| 9 | DNS exfiltration is a technique that attackers use to bypass firewalls by embedding data within DNS queries. | T |
| 10 | A digital forensics investigation can be triggered by corporate policy violations, even if no criminal activity is suspected. | T |

**Essay Questions (10 points):**

1. Explain the one-way hash?

Hash algorithms which map long inputs into a fixed-size output such that it is very difficult (computationally infeasible) to find two different hash inputs that produce the same output.

1. Explain how servers can defend against trial-and-error attacks?

Some steps servers can take:

1. Strong passwords
2. Limit Login Attempts
3. Monitor IP addresses
4. 2FA
5. CAPTCHAs
6. What is the main advantage of using validated tools in a digital forensics investigation?

Digital forensics tools are hardware and software tools that can be used to aid in the recovery and preservation of digital evidence.

1. In the context of digital forensics, describe the process of creating a forensic copy of digital evidence and explain why it is essential to the investigation.

Cloning the digital evidence is a key step in the investigation because it allows forensic investigators to manipulate and test the data without corrupting the original copy.