SECURITY

1. Which of the following is not an example of InfoSec?
2. Data/System is seen only be the authorized people
3. Data/System is changed only as specified by the system
4. Data/System is up when we want it.
5. Data/System gets updated every week.

Hint: We are just concerned with the security of data/system here.

1. Which of the following is one of the CIA Triad?
2. Assurance
3. Confidentiality
4. Information
5. Confidence

Hint: The ‘C’ in CIA.

1. “Guarding against improper information modification or destruction” – Which CIA Triad does this refer to?
2. Confidentiality
3. Integrity
4. Availability
5. Assurance

Hint: ‘Assurance’ is not part of the CIA triad.

1. Which of the following jargons are not defined correctly?
2. Asset: What we’re trying to protect
3. Threat: What we’re protecting against
4. Vulnerability: The people who want to attack us
5. Attack consequence : unauthorized access

Hint: Asset and Threat are defined correctly.

1. Which of the following does not come under the Principle of Easiest Penetration?
2. An intruder can use any available means of penetration.
3. Any system is most vulnerable at its weakest link
4. Attackers will go after the weakest link, not the most obvious link nor the most convenient link to fortify.
5. Cost of security measures should not exceed the value of assets.

Hint: The Principle of Easiest Penetration is associated with the weakest link of a system.

PASSWORDS (113-202)

1. What is Phishing?
2. Attempting to steal user information by disguising malicious content as a trustworthy communication.
3. Monitoring software designed to record keystrokes of a user.
4. Spying on an user in order to obtain personal access information
5. Gaining access of victims documents and only giving it back if ransom is paid.

Hint: Phishing is an example of social engineering(tricking users into believing the hacker is a legitimate agent)

1. What is the minimum number of characters required for a password according to the current NIST password guidelines(if chosen by a human)
2. 6 chars
3. 8 chars
4. 7 chars
5. 9 chars

Hint: 6 chars is the minimum requirement if randomly assigned by a machine.

1. Which of the following passwords would not be blacklisted by the NIST?
2. aaaaaaaa
3. 12345678
4. Password
5. bhjgh@123

Hint: Commonly used passwords get blacklisted by the NIST.

1. Why is it allowed to copy-paste passwords into the password field?
2. Encourages passwords too complex to type
3. This can prevent shoulder-surfing
4. Enables you to type and store all passwords in a single document.
5. This can thwart keyloggers

Hint: This allowance improves safety.

1. Which of the following is the most widely used hash function today?
2. SHA-256
3. SHA-1
4. SHA-3
5. MD5

Hint: The output length is 256 bit.

1. Which of the following password hashing function is described incorrectly?
2. bcrypt: used password as key, encrypts a fixed string repeatedly
3. scrypt: uses memory-hard function to make parallel brute force attacks expensive
4. Argon 2: used password-dependent memory access to thwart time-memory tradeoffs on a GPU.
5. PBKDF2: encodes information into a 128-bit fingerprint.

Hint: bcrypt and scrypt are defined correctly

BIOMETRICS

1. Which of the following is not a type of biometric password?
2. Hand geometry
3. Retinal Pattern
4. Draw-a-secret
5. Voice

Hint: “biometrics” is applying measurements to biology.

1. Which is a phase of biometric authentication?
2. Enrolment
3. Measurement
4. Judgement
5. Management

Hint: The phase where a profile for the user is constructed.

1. Which is not a requirement of Biometric characteristics?
2. Universality
3. Collectability
4. Distinctiveness
5. Versatility

Hint: Collectability and Distinctiveness are requirements.

1. What is False Acceptance Ratio?

a) The rate of system outputting “no match” for wrong input fingerprint.

b) The rate of system outputting “match” for wrong input fingerprint.

c) The rate of system outputting “no match” for correct input fingerprint.

d) The rate of system outputting “match” for correct input fingerprint.

Hint: The answer involves the wrong input fingerprint.

1. How to ensure if a fingerprint isn’t fake?
2. Check for depth of lines
3. Check for perspiration
4. Check for variations in pattern
5. Check for grip

Hint: We check if the finger is “live”.

1. What is a disadvantage of biometric authentication?
2. No need to memorize
3. Cannot be easily shared
4. Cannot be changed
5. Highly identifying

Hint: It is advantageous that biometric authentication is highly identifying and doesn’t need to be shared.

1. What does PII stand for?
2. Personal Information Identification
3. Personally identifiable Information
4. Personality Intrusive Information
5. Privacy Invading Interface

Hint: The ‘I’ stands for information.

1. Which of the following is not a type of web tracker?
2. Cookies
3. Fingerprinters
4. Embedded script
5. Search engines

Hint: A web tracker is a script on websites designed to derive data from you.

1. Which is not true about the Universal Product Code?
2. Number is between 10 to 17 digits long
3. First 6-10 digits represent manufacturer’s identification
4. Next 1-5 represent item number
5. Final digit represents check digit

Hint: The first few numbers represent manufacturer’s identity and the last digit represents check digit.

1. How is the check digit calculated in GTIN-13 system?
2. 3(a2+a4+a6+a8+a10+a12) +a1+a3+a5+a7+a9+a11 mod 10
3. 2(a2+a4+a6+a8+a10+a12) +a1+a3+a5+a7+a9+a11 mod 10
4. 3(a2+a4+a6+a8+a10+a12) + 2(a1+a3+a5+a7+a9+ a11) mod 12
5. a2+a4+a6+a8+a10+a12 +a1+a3+a5+a7+a9+a11 mod 12

Hint: The answer involves taking the modulus of 10.