

Name: _____

2) 23100-1 CYBER SECURITY

1-1 Intro to Security Concepts Worksheet

Assessment Instructions

This is not a quiz, use your notes to complete this worksheet.

Page 1

Question 1 - Multiple Choice

Points: 1

The main goal of computer security is known as:

- | | |
|---------------|--------------|
| A) Prevention | B) Detection |
| C) Protection | D) Response |

Question 2 - Multiple Choice

Points: 1

In the security model equation, which action occurs while a system is running?

- | | |
|---------------|---------------|
| A) Prevention | B) Detection |
| C) Response | D) Protection |

Question 3 - Multiple Choice

Points: 1

The CIA Triad stands for:

- A) Central Intelligence Agency
- B) Confidentiality, Integrity, Availability
- C) Control, Inspect, Access
- D) Cybersecurity, Information, Assets

Question 4 - Multiple Choice

Points: 1

Which CIA principle ensures data is only accessible to authorized users?

- | | |
|--------------------|-------------------|
| A) Integrity | B) Availability |
| C) Confidentiality | D) Authentication |

Question 5 - Multiple Choice

Points: 1

Which CIA principle protects against unauthorized modification of data?

- | | |
|-----------------|--------------------|
| A) Availability | B) Confidentiality |
| C) Encryption | D) Integrity |

Question 6 - Multiple Choice

Points: 1

Data stored on a hard drive or USB is considered:

- | | |
|-----------------|--------------------|
| A) Data in Use | B) Data in Transit |
| C) Data at Rest | D) Active Data |

Question 7 - Multiple Choice

Points: 1

Data being transferred across a network is called:

- | | |
|--------------------|----------------|
| A) Data at Rest | B) Data in Use |
| C) Data in Transit | D) Stored Data |

Question 8 - Multiple Choice

Points: 1

Which example represents a loss of confidentiality?

- A) Website outage from traffic overload
- B) Corrupted database file
- C) Stolen data released to the public
- D) Server hardware failure

Question 9 - Multiple Choice

Points: 1

A Distributed Denial of Service (DDoS) attack primarily impacts:

- | | |
|--------------------|---------------|
| A) Confidentiality | B) Integrity |
| C) Availability | D) Encryption |

Question 10 - Multiple Choice

Points: 1

Which organization created the Cybersecurity Framework mentioned in this unit?

- | | |
|---------|--------|
| A) NSA | B) FBI |
| C) NIST | D) CIA |

Question 11 - Multiple Choice

Points: 1

Which of the following best describes availability?

- A) Keeping data secret
- B) Preventing data changes
- C) Ensuring authorized access when needed
- D) Encrypting stored files

Name: _____

2) 23100-1 CYBER SECURITY
1-2 Authentication Worksheet**Assessment Instructions**

Complete this worksheet online using your notes. The notes can also be available on the link provided in this assignment.

This assignment is due August 25 and closes September 1.

This is not a quiz, use your resources.

Page 1

Question 1 - Multiple Choice

Points: 1

The three A's of security stand for:

- A) Authentication, Access Control, Accounting
- B) Access, Auditing, Assets
- C) Authentication, Authorization, Availability
- D) Authorization, Availability, Auditing

Question 2 - Multiple Choice

Points: 1

Authentication is best described as:

- A) Encrypting information
- B) Tracking user activity
- C) What data you can access
- D) Proving who you are

Question 3 - Multiple Choice

Points: 1

Which of the following is NOT one of the three ways to authenticate?

- A) Something you know
- B) Something you have
- C) Something you share
- D) Something you are

Question 4 - True/False

Points: 1

Authentication establishes trust between two parties.

- A) True
- B) False

Question 5 - Multiple Choice

Points: 1

A password is an example of:

- A) Something you scan
- B) Something you are
- C) Something you have
- D) Something you know

Question 6 - Multiple Choice

Points: 1

A fingerprint is an example of:

- A) Something you type
- B) Something you have
- C) Something you know
- D) Something you are

Question 7 - Multiple Choice

Points: 1

Brute force attacks are best described as:

- A) Physically stealing a device
- B) Trick users into giving passwords
- C) Guessing passwords based on personal info
- D) Testing all possible password combinations

Question 8 - Multiple Choice

Points: 1

Guessing a password based on pet names or birthdays is called:

- A) Stupid user guessing
- B) Brute force
- C) Dictionary attack
- D) Phishing

Question 9 - True/False

Points: 1

Hackers know that many users choose predictable passwords.

- A) True
- B) False

Question 10 - Multiple Choice

Points: 1

Which of the following is considered a weak password practice?

- A) Reusing passwords on important websites
- B) Using uppercase and lowercase letters
- C) Using special characters
- D) Using at least 8 characters

Question 11 - True/False

Points: 1

Strong passwords should be at least 8–10 characters long.

- A) True
- B) False

Question 12 - Multiple Choice

Points: 1

Which password best follows strong password guidelines?

- A) football12
- B) 14t\$24tS32gR
- C) john2006
- D) Password1

Question 13 - True/False

Points: 1

Using personal information in a password makes it easier to guess.

- A) True
- B) False

Question 14 - True/False

Points: 1

Authentication determines what you are allowed to access.

- A) True
- B) False

Question 15 - Multiple Choice

Points: 1

Access control is also known as:

- A) Authentication
- B) Authorization
- C) Auditing
- D) Accounting

Question 16 - True/False

Points: 1

Reusing the same password across multiple sites is recommended.

- A) True
- B) False

Name: _____

2) 23100-1 CYBER SECURITY

1-3 Methods of Authentication Worksheet

Assessment Instructions

Use your notes to complete this assignment.

Page 1

Question 13 - True/False

Points: 1

Two-factor authentication uses more than one method of authentication to increase security.

A) True

B) False

Question 1 - Multiple Choice

Points: 1

Which authentication method is considered "something you have"?

A) Password

B) Fingerprint

C) Smart Card

D) Typing Speed

Question 4 - Multiple Choice

Points: 1

Which of the following is an example of biometric authentication?

A) Security Token

B) Smart Card

C) Password

D) Fingerprint

Question 7 - Multiple Choice

Points: 1

Multi-Factor Authentication (MFA) increases security by:

A) Using longer passwords

B) Changing passwords daily

C) Using more than one authentication method

D) Disabling user accounts

Question 2 - Multiple Choice

Points: 1

What device can detect a smart card or key fob without direct contact?

A) Token

B) Retina Scanner

C) Proximity Reader

D) Certificate

Question 5 - Multiple Choice

Points: 1

Biometric authentication verifies identity using:

A) A secret question

B) A measurable physical characteristic

C) A key fob

D) A certificate

Question 6 - Multiple Choice

Points: 1

One disadvantage of biometric systems is that they can be:

- A) Easy to guess
- B) Expensive to implement
- C) Slow to use passwords
- D) Difficult to replicate

Question 10 - Multiple Choice

Points: 1

Why is an OTP effective against intercepted passwords?

- A) It is used only once
- B) It is stored on a server
- C) It never changes
- D) It is always 20 characters long

Question 3 - Multiple Choice

Points: 1

What do servers commonly use to authenticate remotely with a browser?

- A) PINs
- B) Tokens
- C) Certificates
- D) Fingerprints

Question 9 - Multiple Choice

Points: 1

OTP stands for:

- A) Only Trusted Password
- B) Open Token Process
- C) One Time Password
- D) One Type Protection

Question 11 - Multiple Choice

Points: 1

What is the first recommendation for stopping password attacks?

- A) Avoid MFA
- B) Disable accounts
- C) Remove certificates
- D) Use strong passwords

Question 12 - Multiple Choice

Points: 1

What is the purpose of a lockout after several unsuccessful login attempts?

- A) To stop guessing methods
- B) To make passwords easier to remember
- C) To increase typing speed
- D) To change certificates

Question 8 - Multiple Choice

Points: 1

What is a token?

- A) A browser certificate
- B) A hardware device that changes a code regularly
- C) A fingerprint reader
- D) A password manager

Name: _____

2) 23100-1 CYBER SECURITY
1-4 Password Hashing Worksheet**Page 1****Question 1 - Multiple Choice****Points: 1**

What is the purpose of identity proofing?

- A) To verify identity when a user cannot authenticate
- B) To give immediate access to an account
- C) To hash data
- D) To encrypt data

Question 2 - Multiple Choice**Points: 1**

Which of the following is an example of identity proofing?

- A) Answering a security question
- B) Using a fingerprint scanner
- C) Entering a password
- D) Logging in with SSO

Question 3 - Multiple Choice**Points: 1**

What does Single Sign-On (SSO) allow a user to do?

- A) Reset passwords automatically
- B) Store passwords in plain text
- C) Use multiple passwords
- D) Access many resources after one authentication

Question 4 - Multiple Choice**Points: 1**

A passphrase is:

- A) A stored password file
- B) A type of hash
- C) A string of words that provides strong protection
- D) A short password with symbols

Question 5 - Multiple Choice**Points: 1**

What is hashing?

- A) A type of malware
- B) A one-way mathematical conversion
- C) A two-way encryption process
- D) A password recovery method

Question 6 - Multiple Choice

Points: 1

What is the purpose of a salt in password storage?

- A) Store passwords in plain text
- B) Speed up authentication
- C) Protect against rainbow table attacks
- D) Make passwords shorter

Question 7 - Multiple Choice

Points: 1

A hash collision occurs when:

- A) A password is stored in plain text
- B) A password is forgotten
- C) A hash is deleted
- D) Two different inputs produce the same hash value

Question 8 - True/False

Points: 1

Two different inputs can never create the same hash value.

- A) True
- B) False

Question 9 - True/False

Points: 1

Security questions may be used during identity proofing.

- A) True
- B) False

Question 10 - True/False

Points: 1

A salt helps protect passwords from rainbow table attacks.

- A) True
- B) False

Name: _____

2) 23100-1 CYBER SECURITY
1-5 Malicious Code Cyber Security Worksheet

Page 1

Question 15 - True/False

Points: 1

A RAT is a type of Trojan that installs a backdoor for administrative control over the victim PC.

A) True

B) False

Question 12 - Multiple Choice

Points: 1

What can happen when a worm consumes large amounts of system resources?

A) The operating system may slow down or crash

B) Files are automatically backed up

C) The device becomes faster

D) The firewall is removed

Question 16 - True/False

Points: 1

Logic bombs can be triggered by an external event.

A) True

B) False

Question 3 - Multiple Choice

Points: 1

What is a Zero Day attack?

A) An attack that lasts zero days

B) An attack caused by outdated hardware

C) An attack using very recently discovered code flaws

D) An attack that requires physical access

Question 1 - Multiple Choice

Points: 1

Which is a sign of an APT attack?

A) Increased battery life

B) Off-hours activity showing up in logs

C) Improved network speed

D) Fewer log entries

Question 6 - Multiple Choice

Points: 1

A rootkit allows an attacker to:

A) Improve operating system updates

B) Speed up a computer

C) Gain complete control of a computer

D) Block network traffic

Question 11 - Multiple Choice

Points: 1

What is a worm?

- A) A program that reproduces itself and moves between systems without attaching to a file
- B) A program that creates user accounts
- C) A malicious email message
- D) A form of ransomware

Question 7 - Multiple Choice

Points: 1

What is a logic bomb?

- A) A group of programs installed by an attacker to gain complete control of a computer
- B) A type of firewall
- C) A timed program that performs an operation on a system
- D) A hardware failure

Question 5 - Multiple Choice

Points: 1

The vulnerability window is:

- A) The time it takes to install software
- B) The amount of RAM available
- C) The time before a computer starts up
- D) The time between the start of attacks and the release of a solution

Question 8 - Multiple Choice

Points: 1

A backdoor is designed to:

- A) Improve internet speed
- B) Gain access to a computer
- C) Encrypt data
- D) Remove viruses

Question 13 - Multiple Choice

Points: 1

Which statement about Trojans is TRUE?

- A) They replicate themselves
- B) They usually pretend to do something useful while hiding malicious code
- C) They only affect mobile phones
- D) They are always harmless

Question 10 - Multiple Choice

Points: 1

A virus must:

- A) Use a backdoor
- B) Be downloaded from the internet
- C) Run independently
- D) Attach to another program or executable file

Question 9 - Multiple Choice

Points: 1

What is a virus?

- A) A program that reproduces itself without a host
- B) A program that attaches to a host file to install itself on a system
- C) A hardware device used for security
- D) A program that only steals passwords

Question 4 - Multiple Choice

Points: 1

What is often the best solution for removing a rootkit?

- A) Update antivirus software
- B) Restart the computer
- C) Disconnect from the internet
- D) Wipe the hard drive and reinstall the operating system

Question 17 - True/False

Points: 1

A Zero Day attack targets recently discovered vulnerabilities.

- A) True
- B) False

Question 2 - Multiple Choice

Points: 1

What does APT stand for?

- A) Advanced Persistent Threat
- B) Active Program Tracker
- C) Automated Protection Tool
- D) Authorized Protection Team

Question 14 - True/False

Points: 1

A virus can run completely on its own.

- A) True
- B) False

Name: _____

2) 23100-1 CYBER SECURITY**1-6 Authentication and Password Attacks Worksheet****Page 1****Question 6 - Multiple Choice****Points: 1**

What is credential stuffing?

- A) Creating usernames
- B) Using stolen username/password pairs to access accounts
- C) Sharing passwords with others
- D) Encrypting credentials

Question 1 - Multiple Choice**Points: 1**

What is a database?

- A) A type of malware
- B) A pass the hash attack
- C) A computer password
- D) A collection of data organized for rapid search and retrieval

Question 2 - Multiple Choice**Points: 1**

What is a brute force attack?

- A) Trying every possible combination until the correct password is found
- B) Stealing passwords from a database
- C) A collection of data organized for rapid search and retrieval
- D) Using one password on many accounts

Question 11 - True/False**Points: 1**

Changing compromised passwords can help reduce risk after a breach.

- A) True
- B) False

Question 3 - Multiple Choice**Points: 1**

A dictionary attack works by:

- A) Entering every word in a "dictionary" of potential passwords
- B) Destroying a database
- C) Encrypting passwords
- D) Guessing usernames only

Question 9 - True/False

Points: 1

A database is organized to allow rapid search and retrieval.

A) True

B) False

Question 7 - Multiple Choice

Points: 1

Credential stuffing is successful because many people:

A) Reuse passwords on multiple accounts

B) Use different passwords everywhere

C) Share accounts publicly

D) Avoid online accounts

Question 8 - Multiple Choice

Points: 1

A data breach occurs when:

A) A password is changed

B) A database is exposed, accessed, or stolen

C) A computer is turned off

D) Data is organized

Question 5 - Multiple Choice

Points: 1

Password spraying involves:

A) Creating passwords

B) Resetting passwords

C) Using one weak password on many accounts

D) Trying many passwords on one account

Question 4 - Multiple Choice

Points: 1

A hybrid attack is:

A) A combination of a dictionary attack and brute force attack

B) A type of malware

C) A database breach

D) Trying many passwords on one account

Question 10 - True/False

Points: 1

All data breaches occur because of hackers.

A) True

B) False

