

Name: _____

2) 23100-1 CYBER SECURITY

3-1 System Vulnerabilities Worksheet

Page 1

Question 7 - Multiple Choice**Points: 1**

What helps close a vulnerability?

- A) Installing a patch
- B) Changing your wallpaper
- C) Ignoring updates
- D) Turning off the computer forever

Question 13 - True/False**Points: 1**

Vulnerabilities can never cause financial loss.

- A) True
- B) False

Question 12 - True/False**Points: 1**

Network vulnerabilities are one type of common vulnerability.

- A) True
- B) False

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

A CVE severity score of 10.0 means:

- A) The vulnerability is fixed
- B) The vulnerability is minor
- C) The vulnerability is very severe
- D) The vulnerability is not risky

Question 15 - True/False

Points: 1

A CVE severity score of 0 indicates the highest level of risk.

A) True

B) False

Question 8 - Multiple Choice

Points: 1

MS08-067 had a severity score of 10.0. This means it could:

A) Fix itself automatically

B) Only affect one small program

C) Slightly slow a computer

D) Completely compromise confidentiality, integrity, and availability

Question 10 - Multiple Choice

Points: 1

Why is installing updates important?

A) They remove all files

B) They make your computer heavier

C) They are not important

D) They close vulnerabilities with patches

Question 1 - Multiple Choice

Points: 1

What is a vulnerability?

A) A security flaw, glitch, or weakness that can be exploited

B) A type of antivirus software

C) A software update

D) A secure network connection

Question 11 - Multiple Choice

Points: 1

What does CVE stand for?

-
- A) Critical Validation Environment
- B) Computer Verification Exchange
- C) Cyber Vulnerability Evaluation
- D) Common Vulnerabilities and Exposures

Question 9 - Multiple Choice

Points: 1

What is the best way to research whether a product is secure?

- A) Assume all products are secure
- B) Check the CVE database for known vulnerabilities
- C) Only read random online reviews
- D) Ignore security information

Question 3 - Multiple Choice

Points: 1

What does it mean to mitigate a vulnerability?

- A) Delete the entire system
- B) Make it worse
- C) Minimize the risk or impact
- D) Ignore it

Question 2 - Multiple Choice

Points: 1

What is the purpose of the CVE database?

- A) To store hashed user passwords
- B) To sell security software
- C) To list known vulnerabilities in digital products
- D) To block all hackers

Question 14 - True/False

Points: 1

Every vulnerability listed in the CVE database receives a unique identifier number.

A) True

B) False

Question 4 - Multiple Choice

Points: 1

When a vulnerability is discovered, it is assigned a:

A) IP Address

B) Password

C) Firewall rule

D) CVE identifier number

Question 6 - Multiple Choice

Points: 1

What is an exploit?

A) Code that takes advantage of a vulnerability

B) A secure login method

C) A type of hardware

D) A software update

Name: _____

2) 23100-1 CYBER SECURITY

3-2 System Hardening Worksheet

Page 1

Question 13 - True/False

Points: 1

UAC should be disabled because it is annoying.

A) True

B) False

Question 3 - Multiple Choice

Points: 1

Which tool can be used to identify secure settings needed for an operating system?

A) CIS-CAT

B) Paint

C) Google

D) Microsoft Word

Question 4 - Multiple Choice

Points: 1

Which of the following is a step in system hardening?

A) Disable unnecessary services

B) Turn off Windows Security

C) Remove all applications

D) Delete all user accounts

Question 12 - True/False

Points: 1

Windows updates are one of the most important ways to secure a system.

A) True

B) False

Question 15 - True/False

Points: 1

Having multiple backup copies is known as redundancy.

A) True

B) False

Question 2 - Multiple Choice

Points: 1

What are benchmarks used for in system hardening?

- A) Creating backups
- B) Measuring internet speed
- C) Tracking employee attendance
- D) Providing recommended security configuration settings

Question 5 - Multiple Choice

Points: 1

Which type of update fixes a vulnerability in operating system code to stop exploits?

- A) Hotfix
- B) Critical update
- C) Security update
- D) Driver update

Question 8 - Multiple Choice

Points: 1

What is the purpose of an audit policy?

- A) Install device drivers
- B) Scan for viruses
- C) Back up files
- D) Track actions on the system

Question 6 - Multiple Choice

Points: 1

What does UAC stand for?

- A) Unified Access Control
- B) User Account Connection
- C) User Access Control
- D) User Application Control

Question 9 - Multiple Choice

Points: 1

According to the Least Privilege Principle, users should be given:

- A) The minimum access needed to do their jobs
- B) Full control of all files
- C) Access to every application
- D) Administrative access by default

Question 1 - Multiple Choice

Points: 1

What is system hardening?

- A) Increasing internet speed
- B) Installing new software
- C) Limiting weaknesses that make systems vulnerable to cyberattacks
- D) Creating user accounts

Question 14 - True/False

Points: 1

The least privilege principle says users should have administrator rights whenever possible.

- A) True
- B) False

Question 10 - Multiple Choice

Points: 1

What is the recommended backup strategy?

- A) 6-7 Rule
- B) 2-2-2 Rule
- C) 1-1-1 Rule
- D) 3-2-1 Rule

Question 7 - Multiple Choice

Points: 1

What does an account lockout threshold determine?

- A) Number of failed login attempts allowed
- B) Password length
- C) Audit log storage
- D) Administrator privileges

Question 11 - Multiple Choice

Points: 1

Which statement about backups is true?

- A) A system image includes the operating system and configuration settings
- B) Backups are unnecessary if antivirus software is installed
- C) OneDrive is always a backup
- D) One backup copy is enough

Name: _____

2) 23100-1 CYBER SECURITY
3-3 Threat Modeling & IOT Worksheet

Page 1

Question 7 - Multiple Choice

Points: 1

Threat modeling helps users:

- A) Increase internet speed
- B) Predict the future
- C) Identify and prioritize security risks
- D) Buy new devices

Question 11 - True/False

Points: 1

Threat modeling can be applied to personal devices.

- A) True B) False

Question 9 - Multiple Choice

Points: 1

Why are IoT devices often targeted by cybercriminals?

- A) They are usually unplugged
- B) They are invisible
- C) Many have weak security settings
- D) They cannot connect to networks

Question 3 - Multiple Choice

Points: 1

What is a structured process used to identify that prioritize security risks?

- A) Shodan
- B) Firewall
- C) Internet of Things (IoT)
- D) Threat Modeling
- E) Vulnerability

Question 4 - Multiple Choice

Points: 1

What are physical objects with sensors, software, and internet connectivity?

- A) Threat Modeling
- B) Shodan
- C) Vulnerability
- D) Firewall
- E) Internet of Things (IoT)

Question 13 - True/False

Points: 1

A firewall can help protect a home network.

- A) True
- B) False

Question 10 - Multiple Choice

Points: 1

Which is a recommended way to secure an IoT device?

- A) Use default passwords
- B) Disable all security features
- C) Change the default admin username
- D) Share passwords publicly

Question 1 - Multiple Choice

Points: 1

What is a search engine that gathers information about internet-connected devices?

- A) Vulnerability
- B) Firewall
- C) Shodan
- D) Threat Modeling
- E) Internet of Things (IoT)

Question 6 - Multiple Choice

Points: 1

Which of the following is a reason people often do not secure their devices?

- A) Security updates are always automatic
- B) Their devices are impossible to hack
- C) They enjoy cybersecurity
- D) It can be inconvenient

Question 12 - True/False

Points: 1

The Mirai Botnet used malware to compromise devices.

A) True

B) False

Question 8 - Multiple Choice

Points: 1

Which of the following is an example of an IoT device?

A) Pencil

B) Smart thermostat

C) Textbook

D) Crocs

Question 15 - True/False

Points: 1

The Nest Baby Monitor incident showed that smart devices can be accessed by unauthorized users.

A) True

B) False

Question 14 - True/False

Points: 1

Connecting every IoT device to the internet is always necessary.

A) True

B) False

Question 5 - Multiple Choice

Points: 1

What is a security tool that helps control network traffic?

A) Threat Modeling

B) Firewall

C) Vulnerability

D) Shodan

E) Internet of Things (IoT)

Question 2 - Multiple Choice

Points: 1

What is a weakness that can be exploited by attackers?

- A) Firewall
- B) Internet of Things (IoT)
- C) Vulnerability
- D) Shodan
- E) Threat Modeling