Test Bank for Security Strategies in Windows Platforms and Applications 4th Edition by Shimonski, Solomon

ISBN: 9781284281958

Security Strategies in Windows Platforms and Applications, 4e, ISBN 9781284248999
Robert Shimonski and Michael G. Solomon
Test Bank

Import Settings:
Base Settings: Brownstone Default
Information Field: Complexity
Information Field: Ahead
Information Field: Subject
Information Field: Title
Information Field: Feedback
Information Field: Taxonomy
Information Field: Objective
Highest Answer Letter: D
Multiple Keywords in Same Paragraph: No
NAS ISBN13: 9781284282016, add to Ahead, Title tags

Chapter: Chapter 01 - Quiz

Multiple Choice

1. Which of the following is most likely to be defined as a collection of strategies and controls intended to make a computer environment safe?
A) The confidentiality, availability, and integrity (C-I-A) triad
B) An End-User License Agreement (EULA)
C) Defense in depth
D) Limitation of liabilities
Ans: C
Complexity: Medium
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Information Systems Security” section in the course textbook.
Taxonomy: Understand

2. Which of the following refers to technical controls?
A) Devices or processes that limit logical access to resources
B) Information stored in electronic form on computers
C) Weaknesses that could allow a threat to be realized
D) Written policies, procedures, guidelines, regulations, laws, or rules
Ans: A
Complexity: Easy
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: Technical controls are devices or processes that limit logical access to resources. Examples include user authentication, antivirus software, and firewalls.
Taxonomy: Remember

3. Which type of control includes written policies, procedures, guidelines, regulations, laws, and rules of any kind?
A) Preventive
B) Detective
C) Corrective
D) Administrative
Ans: D
Complexity: Medium
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Information Systems Security” section in the course textbook.
Taxonomy: Remember

4. What is an example of a physical control?
A) Company security policy
B) Firewall rule
C) Fire extinguisher
D) Antivirus software
Ans: C
Complexity: Easy
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: Physical controls are devices that limit access or otherwise protect a resource, such as fences, doors, locks, and fire extinguishers.
Taxonomy: Remember

5. Security controls are commonly classified in which of the following two ways?
A) By what the control is and what it does
B) By what the control is and the type of worker it applies to
C) By what the control does and the level of effort to put the control in place
D) By what the control protects and how long the control is in place
Ans: A
Complexity: Hard
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: There are two common methods for categorizing controls. The first method looks at what the control is. The second method categorizes controls by the type of function they perform—also referred to as what they do.
Taxonomy: Analyze

6. Which of the following best describes confidentiality, availability, and integrity (also known as the C-I-A triad)?
A) Windows threats
B) Tenets of information security

C) Logical controls
D) Physical controls
Ans: B
Complexity: Medium
Ahead: Tenets of Information Security: The C-I-A Triad
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: The practice of securing information involves ensuring three main attributes of information. These three attributes are often called the tenets of information security or the C-I-A triad.
Taxonomy: Understand

7. Which of the following refers to the assurance that information cannot be accessed or viewed by unauthorized users?
A) Integrity
B) Confidentiality
C) Availability
D) Need-to-know
Ans: B
Complexity: Easy
Ahead: Tenets of Information Security: The C-I-A Triad
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Tenets of Information Security: The C-I-A Triad” section in the course textbook.
Taxonomy: Remember

8. Which of the following exists to provide functionality to end users and is often called a customer-facing system?
A) Client
B) Gateway
C) Router
D) Server
Ans: A
Complexity: Easy
Ahead: Mapping Microsoft Windows and Applications into a Typical IT Infrastructure
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Mapping Microsoft Windows and Applications into a Typical IT Infrastructure” section in the course textbook.
Taxonomy: Remember

9. Dafne is an IT manager. She needs to acquire 10 new workstation computers for employee use, each of which will include a web browser, an email client, and an office productivity suite. Which of the following must the computers run?
A) Microsoft Windows Server Standard
B) Microsoft Azure
C) Microsoft Windows (client)

D) Microsoft Windows Server Datacenter
Ans: C
Complexity: Hard
Ahead: Mapping Microsoft Windows and Applications into a Typical IT Infrastructure
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Mapping Microsoft Windows and Applications into a Typical IT Infrastructure” section in the course textbook.
Taxonomy: Apply

10. Alice works in the corporate legal office. The organization recently suffered damages due to a disgruntled employee launching a malware attack on the network that affected Windows installations. Alice is reviewing sections of the Microsoft End-User License Agreement (EULA) to determine whether the cost of Windows licenses can be recovered as a result of the employee’s actions. What section answers Alice’s concerns?
A) Updates
B) Additional Notices—Networks, Data, and Internet Usage
C) Limited Warranty
D) Exclusions from Limited Warranty
Ans: D
Complexity: Hard
Ahead: Microsoft’s End-User License Agreement
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: While the Limited Warranty section of the EULA explains that only the purchase price of Windows can be recovered, regardless of any damages incurred as a result of a Windows fault or incident, the Exclusions from Limited Warranty section explains that the cost of a Windows license cannot be recovered if an organization suffers damages caused by its personnel.
Taxonomy: Analyze

11. What term is best defined as any exposure to a threat?
A) Compromise
B) Vulnerability
C) Risk
D) Weakness
Ans: C
Complexity: Easy
Ahead: Windows Threats and Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Windows Threats and Vulnerabilities” section in the course textbook.
Taxonomy: Understand

12. _____ is defined as one that realizes, or carries out, a threat against vulnerabilities.
A) A risk
B) A weakness
C) A successful attack
D) A control

Ans: C
Complexity: Medium
Ahead: Windows Threats and Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: Once vulnerabilities are discovered, an attacker devises an attack to exploit a weakness. A successful attack is defined as one that realizes, or carries out, a threat against vulnerabilities.
Taxonomy: Understand

13. What are Locky and CryptoLocker examples of?
A) Vulnerabilities
B) Ransomware
C) Technical controls
D) Viruses
Ans: B
Complexity: Easy
Ahead: Anatomy of Microsoft Windows Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Anatomy of Microsoft Windows Vulnerabilities” section in the course textbook.
Taxonomy: Remember

14. Bob is a security analyst scanning for vulnerabilities on a Windows print server. He discovers the print server is vulnerable to the exploit EternalBlue. Which of the following is Bob concerned could exploit this print server?
A) Locky
B) CryptoLocker
C) WannaCry
D) PrintNightmare
Ans: C
Complexity: Medium
Ahead: Anatomy of Microsoft Windows Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: WannaCry used the known exploit called EternalBlue. Locky and CryptoLocker are also ransomware but did not use the exploit EternalBlue. PrintNightmare is not ransomware, but an exploit associated with the Windows print spooler.
Taxonomy: Analyze

15. Your computer network has been successfully attacked. What should you accomplish during the discovery phase of the discovery-analysis-remediation cycle?
A) Consult current vulnerability and security bulletin databases.
B) Implement controls to prevent a recurrence.
C) Determine what “normal” looks like by comparing suspect activity with a baseline.
D) Determine the cause of suspect activity.
Ans: C

Complexity: Hard
Ahead: Discovery-Analysis-Remediation Cycle
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: During the discovery phase, you compare suspect activity with normal activity, often called a baseline. The most common method of accomplishing this is to use activity and monitoring logs.
Taxonomy: Apply

16. Geraldo is an incident response team member. A suspected attack occurred. Geraldo has been monitoring logs for abnormal activity. What is the next step of the discovery-analysis-remediation cycle?
A) Discovery
B) Analyze
C) Remediation
D) Baseline
Ans: B
Complexity: Medium
Ahead: Discovery-Analysis-Remediation Cycle
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: The process for addressing attacks follows a recurring three-step process: discovery, analysis, and remediation. Geraldo's next step is to analyze the system's activity. Analysis may not necessarily indicate an attack but instead point to a cause, such as an unusual workload. Baseline refers to the initial profile of a system's normal activity.
Taxonomy: Apply

17. Which of the following attack types allows an attacker to exploit a system to run malicious code, gain full control of, or further elevate privileges on a vulnerable system?
A) Injection
B) Session hijacking
C) Denial of service
D) Remote code execution
Ans: D
Complexity: Medium
Ahead: Common Forms of Attack
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the "Common Forms of Attack" section in the course textbook.
Taxonomy: Remember

18. Which type of attack generally starts with a message that contains a link or image to click or a file to open?
A) Phishing
B) Denial of service
C) Buffer overflow
D) Packet sniffing
Ans: A

Complexity: Medium
Ahead: Common Forms of Attack
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Common Forms of Attack” section in the course textbook.
Taxonomy: Remember

19. Which of the following describes a family of attacks that depend on the ability to send instructions to a software application that cause the application to carry out unintended actions?
A) Phishing
B) Denial of service
C) Injection
D) Packet sniffing
Ans: C
Complexity: Medium
Ahead: Common Forms of Attack
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Common Forms of Attack” section in the course textbook.
Taxonomy: Remember

20. Erwin is the security analyst for a small company. His logs reveal evidence that a session hijacking attack likely occurred. What is the most likely outcome because of this attack?
A) Users’ credentials might be compromised.
B) Email messages could contain malicious files or links.
C) Malicious tools might be installed on shared drives.
D) Network traffic might be monitored.
Ans: A
Complexity: Hard
Ahead: Common Forms of Attack
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: Session hijacking and credential reuse is an attack form that sets up sessions with valid users. Attackers attempt to take over those valid sessions to capture the credentials and impersonate valid users.
Taxonomy: Analyze

True/False

1. True or False? Logical controls are also called physical controls.
Ans: False
Complexity: Easy
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: Logical controls are also called technical controls.

Taxonomy: Remember

2. True or False? Security controls are mechanisms used to protect information.
Ans: True
Complexity: Easy
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Information Systems Security” section in the course textbook.
Taxonomy: Remember

3. True or False? Security controls can be part of the operating system or application software setup, part of a written policy, or a physical device that limits access to a resource.
Ans: True
Complexity: Medium
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Information Systems Security” section in the course textbook.
Taxonomy: Remember

4. True or False? Detective controls are written policies, procedures, guidelines, regulations, laws, and rules of any kind.
Ans: False
Complexity: Medium
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: Administrative controls are written policies, procedures, guidelines, regulations, laws, and rules of any kind.
Taxonomy: Remember

5. True or False? A firewall is an example of a technical control.
Ans: True
Complexity: Easy
Ahead: Information Systems Security
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Information Systems Security” section in the course textbook.
Taxonomy: Remember

6. True or False? Hacktivists often target victims with the goal of making some sort of social impact.
Ans: True

Complexity: Easy
Ahead: Tenets of Information Security: The C-I-A Triad
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Tenets of Information Security: The C-I-A Triad” section in the course textbook.
Taxonomy: Understand

7. True or False? A mobile device, such as a smartphone, is a type of client system.
Ans: True
Complexity: Easy
Ahead: Mapping Microsoft Windows and Applications into a Typical IT Infrastructure
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Mapping Microsoft Windows and Applications into a Typical IT Infrastructure” section in the course textbook.
Taxonomy: Remember

8. True or False? Server computers provide specific types of services to client applications, either directly or indirectly.
Ans: True
Complexity: Easy
Ahead: Mapping Microsoft Windows and Applications into a Typical IT Infrastructure
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Mapping Microsoft Windows and Applications into a Typical IT Infrastructure” section in the course textbook.
Taxonomy: Understand

9. True or False? Satisfying the C-I-A triad requires more than just implementing controls on a single system.
Ans: True
Complexity: Easy
Ahead: Mapping Microsoft Windows and Applications into a Typical IT Infrastructure
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Mapping Microsoft Windows and Applications into a Typical IT Infrastructure” section in the course textbook.
Taxonomy: Understand

10. True or False? A service level agreement (SLA) is the software license agreement that contains the Microsoft Software License Terms.
Ans: False
Complexity: Medium
Ahead: Microsoft’s End-User License Agreement
Subject: Chapter 1

Title: Microsoft Windows and the Threat Landscape
Feedback: The software license agreement that contains the Microsoft Software License Terms is referred to as the End-User License Agreement (EULA).
Taxonomy: Remember

11. True or False? Attackers look for vulnerabilities, or weaknesses, in an operating system and application software.
Ans: True
Complexity: Easy
Ahead: Windows Threats and Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Windows Threats and Vulnerabilities” section in the course textbook.
Taxonomy: Understand

12. True or False? A vulnerability is defined as any action that could lead to damage, disruption, or loss.
Ans: False
Complexity: Medium
Ahead: Windows Threats and Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: A threat is any action that could lead to damage, disruption, or loss.
Taxonomy: Remember

13. True or False? Not all threats are dangerous.
Ans: True
Complexity: Easy
Ahead: Windows Threats and Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Windows Threats and Vulnerabilities” section in the course textbook.
Taxonomy: Understand

14. True or False? Attackers look for risks to exploit.
Ans: False
Complexity: Easy
Ahead: Windows Threats and Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: Attackers look for vulnerabilities to exploit.
Taxonomy: Understand

15. True or False? In most injection attacks, the attacker encrypts data and demands a payment

using cryptocurrency in exchange for the decryption key.
Ans: False
Complexity: Medium
Ahead: Anatomy of Microsoft Windows Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: In most ransomware attacks, the attacker encrypts data and demands a payment using cryptocurrency in exchange for the decryption key.
Taxonomy: Understand

16. True or False? A denial of service (DoS) attack dramatically slows down or blocks access to one or more resources.
Ans: True
Complexity: Easy
Ahead: Anatomy of Microsoft Windows Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Anatomy of Microsoft Windows Vulnerabilities” section in the course textbook.
Taxonomy: Understand

17. True or False? Cross-site scripting is specially crafted malicious code used to attack web applications.
Ans: True
Complexity: Medium
Ahead: Anatomy of Microsoft Windows Vulnerabilities
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Anatomy of Microsoft Windows Vulnerabilities” section in the course textbook.
Taxonomy: Remember

18. True or False? Security information and event management (SIEM) tools help prepare collected data for correlation and analysis.
Ans: True
Complexity: Medium
Ahead: Discovery-Analysis-Remediation Cycle
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Discovery-Analysis-Remediation Cycle” section in the course textbook.
Taxonomy: Understand

19. True or False? Regarding computer or network attacks, “remediating activity” means to determine that an attack has occurred.
Ans: False
Complexity: Easy

Ahead: Discovery-Analysis-Remediation Cycle
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: Remediating activity means to contain any damage that has occurred, recover from any loss, and implement controls to prevent a recurrence.
Taxonomy: Remember

20. True or False? Packet sniffing is the process of collecting network messages as they travel across a network in hopes of divulging sensitive information, such as passwords.
Ans: True
Complexity: Medium
Ahead: Common Forms of Attack
Subject: Chapter 1
Title: Microsoft Windows and the Threat Landscape
Feedback: See the “Common Forms of Attack” section in the course textbook.
Taxonomy: Understand

