Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Import Settings:
Base Settings: Brownstone Default
Information Field: Complexity
Information Field: Ahead
Information Field: Subject
Information Field: Title
Information Field: Feedback
Information Field: Taxonomy
Highest Answer Letter: D
Multiple Keywords in Same Paragraph: No
NAS ISBN13: 9781284248999, add to Ahead, Title tags

Chapter: Chapter 01 - Quiz

Multiple Choice

1. _____ are people who break the law while hacking or break into systems without authorization.
A) Amateurs
B) Crackers
C) Ethical hackers
D) Ideologues
Ans: B
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: People who break the law or break into systems without authorization are more correctly known as crackers. The media do not usually make the distinction because "hacker" has become such a universal term. In reality, many experienced hackers never break the law and define hacking as producing an outcome that the system's designers never intended or anticipated.
Taxonomy: Remember

2. Which of the following is *not* considered one of the three types of controls used to mitigate risk?
A) Physical
B) Distribution
C) Technical
D) Administrative
Ans: B
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: TAP is an acronym for technical, administrative, and physical, the three types of controls you can use to mitigate risk.
Taxonomy: Remember

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

3. In an organization protecting its IT infrastructure from risks, which control includes firewalls, intrusion prevention systems (IPSs), and biometric authentication?
A) Administrative
B) Physical
C) Technical
D) Vulnerability
Ans: C
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Technical controls take the form of software or hardware devices, such as firewalls, proxies, intrusion detection systems (IDSs), IPSs, biometric authentication, and permissions.
Taxonomy: Remember

4. Which of the following statements is true regarding ethical hackers?
A) Hackers are considered ethical as long as the end result of their actions causes no harm.
B) Ethical hackers believe in the Robin Hood ideal.
C) Ethical hackers can be either white-hat or black-hat hackers.
D) Ethical hackers engage in their activities only with the permission of the asset owner.
Ans: D
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Ethical hackers engage in their activities only with the permission of the asset owner. The permission should be in writing.
Taxonomy: Understand

5. Which of the following refers to the structured and methodical means of investigating, identifying, attacking, and reporting on a target system's strengths and vulnerabilities?
A) Auditing
B) Penetration testing
C) Authentication
D) Reconnaissance
Ans: B
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

6. _____ are specialists in finding software bugs.
A) Crackers
B) Bug bounty hunters
C) Black-box testers
D) Hackers
Ans: B
Complexity: Easy

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: A new range of opportunities exist for people who like to find software bugs. These specialists, called bug bounty hunters, are compensated by software development organizations for the bugs they find before their customers find them.
Taxonomy: Remember

7. The _____ is a major difference between a malicious hacker and an ethical hacker.
A) code of ethics to which each subscribes
B) education level each has obtained
C) level of technological proficiency each has accomplished
D) social position each has reached
Ans: A
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

8. Reconnaissance, scanning, infiltration and escalation, exfiltration, access extension, assault, and obfuscation are considered:
A) hacking steps.
B) antivirus steps.
C) intrusion detection steps.
D) auditing steps.
Ans: A
Complexity: Easy
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Remember

9. Planning, discovery, attack, and reporting are considered:
A) antivirus steps.
B) penetration testing steps.
C) intrusion detection steps.
D) auditing steps.
Ans: B
Complexity: Easy
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: National Institute of Standards and Technology Publication 800-115 (NIST 800-115), "Technical Guide to Information Security Testing and Assessment," describes penetration testing as a four-step process. The steps are planning, discovery, attack, and reporting.
Taxonomy: Remember

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

10. Which hacking methodology is defined as an attacker wanting to cover their tracks by erasing any traces of their presence in the target system?
A) Assault
B) Exfiltration
C) Infiltration and escalation
D) Obfuscation
Ans: D
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: For attackers who want to be clandestine, obfuscation is the phase in which they cover their tracks. With elevated privileges, attackers can often modify log files and other artifacts of their activities or install additional malware to erase any traces of their presence.
Taxonomy: Understand

11. Which type of penetration test is designed to find loopholes or shortcomings in how tasks and operational processes are performed?
A) Administrative attack
B) Physical attack
C) Technical attack
D) Assessment attack
Ans: A
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

12. Which type of penetration test includes anything that targets equipment and facilities with actions such as theft, breaking and entering, or similar actions? It can also include actions against people, such as social engineering–related threats.
A) Administrative attack
B) Physical attack
C) Technical attack
D) Assessment attack
Ans: B
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

13. Of the following, which description best describes the scanning step of hacking?
A) An attacker conducting a ping sweep of all of the victim's known Internet Protocol (IP) addresses
B) An attacker passively acquiring information about the intended victim

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

C) An attacker using acquired information to exploit one or more identified vulnerabilities
D) An attacker using elevated access to extract, modify, or delete sensitive files
Ans: A
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Scanning occurs when an attacker takes the information obtained during the reconnaissance phase and uses it to actively acquire more detailed information about a victim. For example, an attacker might conduct a ping sweep of all the victim's known IP addresses to see which machines respond.
Taxonomy: Understand

14. Violating limits defined by the permitted scope of testing may be sufficient cause for a client _____ against the ethical hacker.
A) to have lack of trust
B) to make an administrative attack
C) to take legal action
D) to write a negative assessment
Ans: C
Complexity: Medium
Ahead: The Role of the Law and Ethical Standards
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Violating limits defined by the permitted scope of testing may be sufficient cause for a client to take legal action against the ethical hacker. In fact, if violating the test scope results in damages, the client may be compelled to take legal action.
Taxonomy: Understand

15. Breaking the trust a client has placed in an ethical hacker can lead to the:
A) planning stage being deemed incomplete.
B) rules of engagement having to be rewritten.
C) questioning of other details, such as the results of the test.
D) failure of the testing results to accurately portray the organization's assets.
Ans: C
Complexity: Medium
Ahead: The Role of the Law and Ethical Standards
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

16. Ryan received a security audit that included a finding that the organization lacked sufficient physical controls in its security program. What action is Ryan most likely to take?
A) Install a new firewall.
B) Upgrade an existing fence.
C) Enhance an existing policy.
D) Upgrade existing encryption.
Ans: B
Complexity: Medium
Ahead: Profiles and Motives of Different Types of Hackers

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Physical controls protect assets from traditional threats such as theft or vandalism. Such controls include door locks, lighting, and fences.
Taxonomy: Apply

17. Maria is conducting a security investigation and has identified a suspect. The suspect is an employee of the organization who had access to a server file share containing sensitive information. The employee routinely accesses that share during the normal course of business but is suspected of stealing sensitive information from it and sending it to a competitor. Which element of a crime has Maria *not* yet established?
A) Motive
B) Opportunity
C) Means
D) Ownership
Ans: A
Complexity: Medium
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Maria has established the suspect has the opportunity by identifying that the suspect had access to the file share. She demonstrated means by showing that the attacker accessed the share in the past. She has not yet established a motive for the crime. Ownership is not one of the three elements of a crime.
Taxonomy: Analyze

18. Harry is planning to hire a consultant to perform a penetration test. He would like the test to be announced in advance to the testing team. What is this type of testing called?
A) White box
B) Grey box
C) Red box
D) Black box
Ans: A
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: In white-box testing, advance knowledge is provided to the testing team.
Taxonomy: Apply

19. Acme Widgets recently experienced an attack in which the attacker broke into a file server and modified protected data. Which of the following is a goal of information security that was violated?
A) Integrity
B) Availability
C) Disclosure
D) Confidentiality
Ans: A
Complexity: Hard
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Title: Hacking: The Next Generation
Feedback: This attack modified protected data, violating the integrity of the data, which should only have been changed by authorized personnel.
Taxonomy: Analyze

20. Gwen is investigating a security incident. She discovered that an attacker has deleted the boot files on a number of critical servers, making it impossible to boot the machines. What phase of an attack is this?
A) Reconnaissance
B) Infiltration
C) Exfiltration
D) Assault
Ans: D
Complexity: Hard
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: During the assault phase, the attacker can remove or modify configuration or other files on a computer, causing it to change the way it operates, including causing it to fail to boot.
Taxonomy: Apply

True/False

1. True or False? Nation-state actors are extremely sophisticated, have large budgets, and are tasked with carrying out cyberwarfare operations.
Ans: True
Complexity: Medium
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

2. True or False? The Robin Hood ideal is a hacker justification for stealing software and other media from "rich" companies and delivering them to "poor" consumers.
Ans: True
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

3. True or False? Whereas the primary goal of a penetration test is to determine whether a specific resource can be compromised, a vulnerability assessment is a survey of a system to identify as many vulnerabilities as possible.

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Ans: True
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

4. True or False? Policies and procedures are forms of technical controls.
Ans: False
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Administrative controls take the form of policies and procedures.
Taxonomy:

5. True or False? A vulnerability refers to a piece of software, a tool, or a technique that targets or takes advantage of a vulnerability, leading to privilege escalation, loss of integrity or confidentiality, or denial of service on a computer system or resource.
Ans: False
Complexity: Hard
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: An exploit refers to a piece of software, a tool, or a technique that targets or takes advantage of a vulnerability, leading to privilege escalation, loss of integrity or confidentiality, or denial of service on a computer system or resource.
Taxonomy:

6. True or False? White-hat hackers are sometimes referred to as ethical hackers.
Ans: True
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

7. True or False? Some hackers believe that it is okay to commit a crime as long as one is doing it to learn.
Ans: True
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

8. True or False? The hacking community engages in more "lone wolf" types of hacking activities as opposed to working as teams.
Ans: False
Complexity: Medium
Ahead: A Look at the History of Computer Hacking
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: In the past, it was normal for a "lone wolf" type to engage in hacking activities. Today, a new pattern of a collective or group effort has emerged.
Taxonomy:

9. True or False? Three primary things are needed to commit a crime: means, motive, and opportunity.
Ans: True
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

10. True or False? Penetration testing involves simulating an attack in order to determine what would happen to an organization if an actual attack occurred.
Ans: True
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

11. True or False? In black-box penetration testing, advanced knowledge is provided to the testing team.
Ans: False
Complexity: Easy
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Black-box testing is most often used when an organization wants to closely simulate how an attacker views a system, so no knowledge of the system is provided to the testing team.
Taxonomy:

12. True or False? During the infiltration and escalation phase of a hacking attack, the attacker attempts to exploit one or more identified vulnerabilities.
Ans: True
Complexity: Medium
Ahead: Common Hacking Methodologies

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

13. True or False? The more secure a system becomes, the more convenient it tends to be.
Ans: False
Complexity: Easy
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Security and convenience are often in conflict with one another. The more secure a system becomes, the less convenient it tends to be.
Taxonomy:

14. True or False? The C-I-A triad involves disclosure, alternation, and disruption.
Ans: False
Complexity: Easy
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: In opposition to the confidentiality, integrity, and availability (C-I-A) triad, the anti-triad involves disclosure, alternation, and disruption.
Taxonomy:

15. True or False? In the ethical hacking and security process, all assets are considered to have equal value for an organization.
Ans: False
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Part of ethical hacking is identifying assets, risks, vulnerabilities, and threats. From an InfoSec perspective, not all assets are created equal and do not have equal value for an organization.
Taxonomy:

16. True or False? It is possible for a penetration test to result in systems or services shutting down and completely stopping a company's operations.
Ans: True
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

17. True or False? Penetration testing requires rules to be agreed upon in advance.
Ans: True
Complexity: Easy
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

18. True or False? Ethical hacking does not always require the explicit permission of the owner of the target.
Ans: False
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Engaging in any hacking activity without the explicit permission of the owner of the target is a crime, whether the hacker is caught or not.
Taxonomy:

19. True or False? Two important points when considering exceeding the scope of ethical hacking or violating the stated guidelines are trust and legal implications.
Ans: True
Complexity: Medium
Ahead: The Role of the Law and Ethical Standards
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

20. True or False? Because of the nature of the Internet and computer crime, it is possible for any given crime to stretch over multiple local and international jurisdictions.
Ans: True
Complexity: Medium
Ahead: The Role of the Law and Ethical Standards
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Multiple Choice

1. _____ are people who break the law while hacking or break into systems without authorization.
A) Amateurs
B) Crackers
C) Ethical hackers
D) Ideologues

Ans: B
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: People who break the law or break into systems without authorization are more correctly known as crackers. The media do not usually make the distinction because "hacker" has become such a universal term. In reality, many experienced hackers never break the law and define hacking as producing an outcome that the system's designers never intended or anticipated.
Taxonomy: Remember

2. Which of the following is *not* considered one of the three types of controls used to mitigate risk?
A) Physical
B) Distribution
C) Technical
D) Administrative

Ans: B
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: TAP is an acronym for technical, administrative, and physical, the three types of controls you can use to mitigate risk.
Taxonomy: Remember

3. In an organization protecting its IT infrastructure from risks, which control includes firewalls, intrusion prevention systems (IPSs), and biometric authentication?
A) Administrative

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

B) Physical
C) Technical
D) Vulnerability

Ans: C
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Technical controls take the form of software or hardware devices, such as firewalls, proxies, intrusion detection systems (IDSs), IPSs, biometric authentication, and permissions.
Taxonomy: Remember

4. Which of the following statements is true regarding ethical hackers?
A) Hackers are considered ethical as long as the end result of their actions causes no harm.
B) Ethical hackers believe in the Robin Hood ideal.
C) Ethical hackers can be either white-hat or black-hat hackers.
D) Ethical hackers engage in their activities only with the permission of the asset owner.

Ans: D
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Ethical hackers engage in their activities only with the permission of the asset owner. The permission should be in writing.
Taxonomy: Understand

5. Which of the following refers to the structured and methodical means of investigating, identifying, attacking, and reporting on a target system's strengths and vulnerabilities?
A) Auditing
B) Penetration testing
C) Authentication
D) Reconnaissance

Ans: B
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

6. _____ are specialists in finding software bugs.
A) Crackers
B) Bug bounty hunters
C) Black-box testers
D) Hackers

Ans: B
Complexity: Easy
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: A new range of opportunities exist for people who like to find software bugs. These specialists, called bug bounty hunters, are compensated by software development organizations for the bugs they find before their customers find them.
Taxonomy: Remember

7. The _____ is a major difference between a malicious hacker and an ethical hacker.
A) code of ethics to which each subscribes
B) education level each has obtained
C) level of technological proficiency each has accomplished
D) social position each has reached

Ans: A
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

8. Reconnaissance, scanning, infiltration and escalation, exfiltration, access extension, assault, and obfuscation are considered:
A) hacking steps.
B) antivirus steps.
C) intrusion detection steps.
D) auditing steps.

Ans: A
Complexity: Easy

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Remember

9. Planning, discovery, attack, and reporting are considered:
A) antivirus steps.
B) penetration testing steps.
C) intrusion detection steps.
D) auditing steps.

Ans: B
Complexity: Easy
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: National Institute of Standards and Technology Publication 800-115 (NIST 800-115), "Technical Guide to Information Security Testing and Assessment," describes penetration testing as a four-step process. The steps are planning, discovery, attack, and reporting.
Taxonomy: Remember

10. Which hacking methodology is defined as an attacker wanting to cover their tracks by erasing any traces of their presence in the target system?
A) Assault
B) Exfiltration
C) Infiltration and escalation
D) Obfuscation

Ans: D
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: For attackers who want to be clandestine, obfuscation is the phase in which they cover their tracks. With elevated privileges, attackers can often modify log files and other artifacts of their activities or install additional malware to erase any traces of their presence.
Taxonomy: Understand

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

11. Which type of penetration test is designed to find loopholes or shortcomings in how tasks and operational processes are performed?
A) Administrative attack
B) Physical attack
C) Technical attack
D) Assessment attack

Ans: A
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

12. Which type of penetration test includes anything that targets equipment and facilities with actions such as theft, breaking and entering, or similar actions? It can also include actions against people, such as social engineering–related threats.
A) Administrative attack
B) Physical attack
C) Technical attack
D) Assessment attack

Ans: B
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

13. Of the following, which description best describes the scanning step of hacking?
A) An attacker conducting a ping sweep of all of the victim's known Internet Protocol (IP) addresses
B) An attacker passively acquiring information about the intended victim
C) An attacker using acquired information to exploit one or more identified vulnerabilities
D) An attacker using elevated access to extract, modify, or delete sensitive files

Ans: A
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Title: Hacking: The Next Generation
Feedback: Scanning occurs when an attacker takes the information obtained during the reconnaissance phase and uses it to actively acquire more detailed information about a victim. For example, an attacker might conduct a ping sweep of all the victim's known IP addresses to see which machines respond.
Taxonomy: Understand

14. Violating limits defined by the permitted scope of testing may be sufficient cause for a client _____ against the ethical hacker.
A) to have lack of trust
B) to make an administrative attack
C) to take legal action
D) to write a negative assessment

Ans: C
Complexity: Medium
Ahead: The Role of the Law and Ethical Standards
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Violating limits defined by the permitted scope of testing may be sufficient cause for a client to take legal action against the ethical hacker. In fact, if violating the test scope results in damages, the client may be compelled to take legal action.
Taxonomy: Understand

15. Breaking the trust a client has placed in an ethical hacker can lead to the:
A) planning stage being deemed incomplete.
B) rules of engagement having to be rewritten.
C) questioning of other details, such as the results of the test.
D) failure of the testing results to accurately portray the organization's assets.

Ans: C
Complexity: Medium
Ahead: The Role of the Law and Ethical Standards
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy: Understand

16. Ryan received a security audit that included a finding that the organization lacked sufficient physical controls in its security program. What action is Ryan most likely to take?

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

A) Install a new firewall.
B) Upgrade an existing fence.
C) Enhance an existing policy.
D) Upgrade existing encryption.

Ans: B
Complexity: Medium
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Physical controls protect assets from traditional threats such as theft or vandalism. Such controls include door locks, lighting, and fences.
Taxonomy: Apply

17. Maria is conducting a security investigation and has identified a suspect. The suspect is an employee of the organization who had access to a server file share containing sensitive information. The employee routinely accesses that share during the normal course of business but is suspected of stealing sensitive information from it and sending it to a competitor. Which element of a crime has Maria *not* yet established?
A) Motive
B) Opportunity
C) Means
D) Ownership

Ans: A
Complexity: Medium
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Maria has established the suspect has the opportunity by identifying that the suspect had access to the file share. She demonstrated means by showing that the attacker accessed the share in the past. She has not yet established a motive for the crime. Ownership is not one of the three elements of a crime.
Taxonomy: Analyze

18. Harry is planning to hire a consultant to perform a penetration test. He would like the test to be announced in advance to the testing team. What is this type of testing called?
A) White box
B) Grey box
C) Red box
D) Black box

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Ans: A
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: In white-box testing, advance knowledge is provided to the testing team.
Taxonomy: Apply

19. Acme Widgets recently experienced an attack in which the attacker broke into a file server and modified protected data. Which of the following is a goal of information security that was violated?
A) Integrity
B) Availability
C) Disclosure
D) Confidentiality

Ans: A
Complexity: Hard
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: This attack modified protected data, violating the integrity of the data, which should only have been changed by authorized personnel.
Taxonomy: Analyze

20. Gwen is investigating a security incident. She discovered that an attacker has deleted the boot files on a number of critical servers, making it impossible to boot the machines. What phase of an attack is this?
A) Reconnaissance
B) Infiltration
C) Exfiltration
D) Assault

Ans: D
Complexity: Hard
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: During the assault phase, the attacker can remove or modify configuration or other files on a computer, causing it to change the way it operates, including causing it to fail to boot.
Taxonomy: Apply

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

True/False

1. True or False? Nation-state actors are extremely sophisticated, have large budgets, and are tasked with carrying out cyberwarfare operations.

Ans: True
Complexity: Medium
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

2. True or False? The Robin Hood ideal is a hacker justification for stealing software and other media from "rich" companies and delivering them to "poor" consumers.

Ans: True
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

3. True or False? Whereas the primary goal of a penetration test is to determine whether a specific resource can be compromised, a vulnerability assessment is a survey of a system to identify as many vulnerabilities as possible.

Ans: True
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

4. True or False? Policies and procedures are forms of technical controls.

Ans: False
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Administrative controls take the form of policies and procedures.
Taxonomy:

5. True or False? A vulnerability refers to a piece of software, a tool, or a technique that targets or takes advantage of a vulnerability, leading to privilege escalation, loss of integrity or confidentiality, or denial of service on a computer system or resource.

Ans: False
Complexity: Hard
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: An exploit refers to a piece of software, a tool, or a technique that targets or takes advantage of a vulnerability, leading to privilege escalation, loss of integrity or confidentiality, or denial of service on a computer system or resource.
Taxonomy:

6. True or False? White-hat hackers are sometimes referred to as ethical hackers.

Ans: True
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

7. True or False? Some hackers believe that it is okay to commit a crime as long as one is doing it to learn.

Ans: True
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

8. True or False? The hacking community engages in more "lone wolf" types of hacking activities as opposed to working as teams.

Ans: False
Complexity: Medium
Ahead: A Look at the History of Computer Hacking
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: In the past, it was normal for a "lone wolf" type to engage in hacking activities. Today, a new pattern of a collective or group effort has emerged.
Taxonomy:

9. True or False? Three primary things are needed to commit a crime: means, motive, and opportunity.

Ans: True
Complexity: Easy
Ahead: Profiles and Motives of Different Types of Hackers
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

10. True or False? Penetration testing involves simulating an attack in order to determine what would happen to an organization if an actual attack occurred.

Ans: True
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

11. True or False? In black-box penetration testing, advanced knowledge is provided to the testing team.

Ans: False
Complexity: Easy
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Black-box testing is most often used when an organization wants to closely simulate how an attacker views a system, so no knowledge of the system is provided to the testing team.
Taxonomy:

12. True or False? During the infiltration and escalation phase of a hacking attack, the attacker attempts to exploit one or more identified vulnerabilities.

Ans: True
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

13. True or False? The more secure a system becomes, the more convenient it tends to be.

Ans: False
Complexity: Easy
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Security and convenience are often in conflict with one another. The more secure a system becomes, the less convenient it tends to be.
Taxonomy:

14. True or False? The C-I-A triad involves disclosure, alternation, and disruption.

Ans: False
Complexity: Easy
Ahead: Ethical Hacking and Penetration Testing

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: In opposition to the confidentiality, integrity, and availability (C-I-A) triad, the anti-triad involves disclosure, alternation, and disruption.
Taxonomy:

15. True or False? In the ethical hacking and security process, all assets are considered to have equal value for an organization.

Ans: False
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Part of ethical hacking is identifying assets, risks, vulnerabilities, and threats. From an InfoSec perspective, not all assets are created equal and do not have equal value for an organization.
Taxonomy:

16. True or False? It is possible for a penetration test to result in systems or services shutting down and completely stopping a company's operations.

Ans: True
Complexity: Medium
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

17. True or False? Penetration testing requires rules to be agreed upon in advance.

Ans: True
Complexity: Easy
Ahead: Common Hacking Methodologies
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon

18. True or False? Ethical hacking does not always require the explicit permission of the owner of the target.

Ans: False
Complexity: Medium
Ahead: Ethical Hacking and Penetration Testing
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback: Engaging in any hacking activity without the explicit permission of the owner of the target is a crime, whether the hacker is caught or not.
Taxonomy:

19. True or False? Two important points when considering exceeding the scope of ethical hacking or violating the stated guidelines are trust and legal implications.

Ans: True
Complexity: Medium
Ahead: The Role of the Law and Ethical Standards
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

20. True or False? Because of the nature of the Internet and computer crime, it is possible for any given crime to stretch over multiple local and international jurisdictions.

Ans: True
Complexity: Medium
Ahead: The Role of the Law and Ethical Standards
Subject: Chapter 1
Title: Hacking: The Next Generation
Feedback:
Taxonomy:

Copyright © 2024 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

Access Complete Test Bank for Ethical Hacking - Techniques Tools and Countermeasures 4th Solomon