Test Exam – Cybersecurity

PRACTICE EXAM TEST

Cristian Villegas Aparicio

GITHUB | LINKEDIN

Cybersecurity Essentials:

NEW QUESTION 1
What does the term "Phishing" refer to in the context of cybersecurity?

A. A method of securing network communication
B. Sending malicious emails to trick individuals into revealing sensitive information
C. The process of encrypting data to protect it from unauthorized access
D. A type of firewall configuration

Answer: B

NEW QUESTION 2
In the context of cybersecurity, what is the purpose of a firewall?

A. To protect against physical break-ins
B. To monitor website traffic
C. To prevent unauthorized access to or from a private network
D. To scan for viruses on a computer

Answer: C

NEW QUESTION 3
What is the purpose of a Virtual Private Network (VPN) in cybersecurity?

A. Encrypting internet traffic for enhanced security
B. Enhancing physical security within an office
C. Blocking access to certain websites
D. Monitoring user activity on the network

Answer: A

NEW QUESTION 4
Which of the following are common social engineering techniques? (Select two)

A. Phishing
B. Encryption
C. Firewall Configuration
D. Biometric Authentication

Answer: A D

MITRE ATT&CK Framework:

NEW QUESTION 5
What does MITRE ATT&CK stand for?

A. Advanced Threat Techniques & Counter Knowledge
B. Mitigation Techniques for Attack and Counter Knowledge
C. Adversarial Tactics, Techniques, and Common Knowledge
D. Malicious Intrusion and Threat Elimination

Answer: C

NEW QUESTION 6
In the MITRE ATT&CK Matrix, what does the "Execution" tactic focus on?

A. Techniques that result in actions being taken
B. Methods to evade detection
C. Strategies for lateral movement
D. Procedures for privilege escalation

Answer: A

NEW QUESTION 7
Select the techniques associated with the "Credential Access" tactic in MITRE ATT&CK. (Select two)

A. Credential Dumping
B. Exfiltration
C. Defense Evasion
D. Discovery

Answer: A B

NEW QUESTION 8
Which of the following are considered privilege escalation techniques? (Select two)

A. Spear Phishing
B. Exploitation of Software Vulnerabilities
C. Pass-the-Hash
D. VPN Configuration

Answer: B C

Threat Intelligence:

NEW QUESTION 9
What is the main goal of Threat Intelligence in cybersecurity?

A. To encrypt sensitive data
B. To analyze and understand potential threats
C. To build a secure firewall
D. To detect and remove viruses

Answer: B

NEW QUESTION 10
How can organizations benefit from sharing threat intelligence?

A. By slowing down incident response
B. By fostering collaboration and improving overall cybersecurity
C. By increasing the complexity of network defenses
D. By keeping threats confidential within the organization

Answer: B

NEW QUESTION 11
What types of threat intelligence can organizations leverage? (Select two)

A. Tactical Intelligence
B. Strategic Intelligence
C. Antivirus Signatures
D. Physical Security Measures

Answer: A B

NEW QUESTION 12
Identify the benefits of Threat Intelligence sharing. (Select two)

A. Increased Isolation of Networks
B. Enhanced Collaboration and Collective Defense
C. Reduced Complexity of Security Solutions
D. Internalization of Threats

Answer: B C

Risk Management:

NEW QUESTION 13

What is the primary purpose of a risk assessment in cybersecurity?

A. To eliminate all risks
B. To identify and prioritize potential risks
C. To install antivirus software
D. To create a backup of data

Answer: B

NEW QUESTION 14

In risk management, what is the "residual risk"?

A. The risk that remains after implementing risk mitigation strategies
B. The initial level of risk before any assessment
C. The risk associated with new technologies
D. The risk of physical damage to hardware

Answer: A

NEW QUESTION 15

What are examples of risk mitigation strategies? (Select two)

A. Regular Data Backups
B. Risk Acceptance
C. Increased Network Complexity
D. Security Awareness Training

Answer: A D

NEW QUESTION 16

Select the elements considered in a risk assessment. (Select two)

A. Impact
B. Antivirus Software
C. Probability
D. Physical Access Controls

Answer: A C

Incident Lifecycle:

NEW QUESTION 17
What are the key stages of the incident response lifecycle?

A. Detection, Prevention, Recovery
B. Identification, Containment, Eradication, Recovery, Lessons Learned
C. Firewall, Antivirus, Encryption
D. Assessment, Authorization, Audit

Answer: B

NEW QUESTION 18
What is the primary goal during the "Containment" phase of the incident response lifecycle?

A. To identify the root cause of the incident
B. To limit the impact and prevent further damage
C. To recover lost data
D. To communicate with stakeholders

Answer: B

NEW QUESTION 19
What actions are typically performed during the "Recovery" phase of the incident response lifecycle? (Select two)

A. Analyzing Indicators of Compromise (IoCs)
B. Identifying the Attacker
C. Restoring Systems to Normal Operation
D. Implementing Additional Security Controls

Answer: C D

NEW QUESTION 20
Identify the goals of the "Lessons Learned" phase in incident response. (Select two)

A. Identifying Gaps in Security Controls
B. Assigning Blame for the Incident
C. Enhancing Incident Detection Capabilities

D. Ignoring the Incident Entirely

Answer: A C