cyber security fundamentals 2020 exam answers

Cyber security fundamentals 2020 exam answers are crucial for individuals and organizations aiming to build robust defenses against the ever-evolving landscape of cyber threats. Understanding these fundamental concepts is not just about passing an exam; it's about establishing a foundational knowledge base to protect sensitive data, maintain operational continuity, and ensure compliance with industry regulations. This comprehensive guide delves into the core principles of cybersecurity, offering insights into common exam topics and providing a framework for grasping essential security measures. We'll explore critical areas such as threat identification, risk management, security controls, and incident response, all designed to equip you with the knowledge needed to navigate the complexities of the digital security world. Whether you're preparing for certification or seeking to enhance your organization's security posture, this article serves as your definitive resource for cybersecurity fundamentals.

Understanding the Cybersecurity Landscape

The digital realm is constantly expanding, bringing with it an unprecedented surge in the volume and sophistication of cyber threats. Understanding the current cybersecurity landscape is paramount for anyone seeking to grasp the nuances of **cyber security fundamentals 2020 exam answers**. This involves recognizing the actors involved, their motivations, and the ever-changing tactics, techniques, and procedures (TTPs) they employ. From nation-state sponsored attacks aimed at critical infrastructure to opportunistic cybercriminals seeking financial gain through ransomware and phishing, the threat landscape is diverse and dynamic. Organizations must be acutely aware of these evolving threats to implement effective security strategies.

The year 2020 presented a unique set of challenges and opportunities in cybersecurity, largely influenced by global events that accelerated digital transformation. The shift to remote work, increased reliance on cloud services, and the proliferation of interconnected devices (IoT) created new attack vectors and expanded the attack surface. Understanding these contextual shifts is vital for comprehending the types of questions that might appear on a **cyber security fundamentals 2020 exam**, as it reflects the prevailing concerns and priorities of the time.

Key Concepts in Cyber Security Fundamentals

At the heart of cybersecurity are several foundational principles that underpin all security efforts. Mastering these concepts is essential for anyone preparing for a **cyber security fundamentals 2020 exam**. These principles guide the development and implementation of security measures, ensuring a comprehensive approach to protecting digital assets.

The CIA Triad: Confidentiality, Integrity, and Availability

The CIA triad is a cornerstone of information security. Understanding each element and how they interrelate is critical for grasping cybersecurity principles.

- **Confidentiality:** Ensures that information is accessible only to those authorized to have access. This is often achieved through encryption, access controls, and authentication mechanisms. The goal is to prevent unauthorized disclosure of sensitive data.
- **Integrity:** Guarantees that information is accurate, complete, and has not been altered or destroyed in an unauthorized manner. This is typically maintained through hashing algorithms, digital signatures, and access controls to prevent unauthorized modifications.
- **Availability:** Assures that authorized users can access information and resources when they need them. This involves robust infrastructure, disaster recovery plans, and measures to protect against denial-of-service (DoS) attacks.

Authentication, Authorization, and Accounting (AAA)

AAA protocols are fundamental to managing user access and ensuring accountability within a network or system.

- **Authentication:** The process of verifying the identity of a user, system, or service. This can involve passwords, multi-factor authentication (MFA), biometrics, or digital certificates.
- **Authorization:** Once authenticated, authorization determines what actions an authenticated entity is permitted to perform. This involves assigning roles and permissions based on the principle of least privilege.
- **Accounting:** The process of tracking and recording user activities and system events. This provides an audit trail, which is crucial for security monitoring, forensics, and compliance.

Least Privilege

The principle of least privilege dictates that users, programs, or processes should only have the minimum level of access and permissions necessary to perform their intended functions. This minimizes the potential damage if an account is compromised or a program malfunctions.

Defense in Depth

Defense in depth is a security strategy that employs multiple layers of security controls. The idea is that if one security measure fails, others are in place to prevent or mitigate the impact of a breach. This layered approach provides a more robust security posture.

Common Threats and Vulnerabilities

Identifying and understanding common threats and vulnerabilities is a core component of **cyber security fundamentals 2020 exam answers**. Knowledge of these risks allows for proactive defense strategies.

Malware

Malware, short for malicious software, is designed to infiltrate, damage, or gain unauthorized access to computer systems. Common forms include viruses, worms, Trojans, ransomware, spyware, and adware.

- **Viruses:** Attach themselves to legitimate files and require user action to spread.
- **Worms:** Self-replicating and can spread across networks without user intervention.
- **Trojans:** Disguised as legitimate software, they can create backdoors, steal data, or damage systems.
- **Ransomware:** Encrypts a victim's files and demands a ransom payment for their decryption.
- **Spyware:** Secretly monitors user activity and collects personal information.

Phishing and Social Engineering

Phishing attacks and social engineering tactics exploit human psychology to trick individuals into divulging sensitive information or performing actions that compromise security. These attacks often appear legitimate, impersonating trusted entities like banks or well-known companies.

- **Phishing:** Typically conducted via email, aiming to steal credentials, credit card numbers, or other personal information.
- **Spear Phishing:** A more targeted form of phishing, directed at specific individuals or organizations.
- **Whaling:** Spear phishing attacks targeting senior executives or high-profile individuals.
- **Pretexting:** Creating a fabricated scenario (pretext) to gain trust and elicit information.
- **Baiting:** Offering a tempting enticement (e.g., a free download) that, when acted upon, delivers malware.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

These attacks aim to disrupt the normal functioning of a server, service, or network by overwhelming it with a flood of traffic or requests. A DDoS attack utilizes multiple compromised systems to launch the attack simultaneously, making it more difficult to mitigate.

Man-in-the-Middle (MitM) Attacks

In a MitM attack, an attacker intercepts communications between two parties, potentially eavesdropping on or altering the content of the messages without either party's knowledge. This is particularly dangerous on unsecured networks.

Zero-Day Exploits

Zero-day exploits target vulnerabilities in software or hardware that are unknown to the vendor or the public. Because there are no patches or defenses available, these exploits are particularly dangerous.

Essential Security Controls and Best Practices

Implementing robust security controls and adhering to best practices are vital for building a strong cybersecurity foundation, a key area for **cyber security fundamentals 2020 exam answers**.

Access Control Mechanisms

Controlling who can access what resources is fundamental. This includes authentication and authorization measures discussed earlier.

- **Role-Based Access Control (RBAC):** Assigns permissions based on user roles rather than individual users.
- **Attribute-Based Access Control (ABAC):** Uses policies that define access based on a combination of attributes of the user, resource, and environment.
- **Multi-Factor Authentication (MFA):** Requires users to provide two or more forms of verification before granting access, significantly enhancing security.

Encryption

Encryption is the process of converting data into a code to prevent unauthorized access. It's crucial for protecting data both at rest (stored) and in transit (being transmitted).

- **Symmetric Encryption:** Uses a single key for both encryption and decryption.

- **Asymmetric Encryption:** Uses a pair of keys – a public key for encryption and a private key for decryption.
- **Hashing:** A one-way process that converts data into a fixed-size string of characters, used for data integrity verification.

Patch Management

Regularly updating software and systems with security patches is critical to fix known vulnerabilities. An effective patch management program ensures that systems are protected against newly discovered threats.

Endpoint Security

Protecting individual devices like laptops, desktops, and mobile phones is essential. This includes antivirus software, endpoint detection and response (EDR) solutions, and device hardening.

Security Awareness Training

Human error is often a significant factor in security breaches. Comprehensive security awareness training for all employees can help them recognize and avoid threats like phishing and social engineering.

Risk Management and Compliance

Effective cybersecurity requires a structured approach to identifying, assessing, and mitigating risks, as well as adhering to relevant regulations. These aspects are often tested in **cyber security fundamentals 2020 exam answers**.

Risk Assessment

Risk assessment involves identifying potential threats, analyzing their likelihood of occurrence, and determining the potential impact on an organization. This helps prioritize security efforts.

- **Threat Identification:** Identifying all potential sources of harm.
- **Vulnerability Identification:** Pinpointing weaknesses in systems, processes, or controls.

- **Risk Analysis:** Quantifying or qualifying the level of risk based on likelihood and impact.
- **Risk Evaluation:** Comparing the analyzed risk against risk criteria to determine if it is acceptable.

Risk Mitigation

Once risks are identified and assessed, strategies are developed to reduce or eliminate them. This can involve implementing controls, transferring risk (e.g., through insurance), or accepting the risk if it is within acceptable limits.

Compliance and Regulations

Organizations must comply with various data protection and privacy regulations, which vary by industry and geographical location. Understanding these requirements is crucial.

- **GDPR (General Data Protection Regulation):** A comprehensive data protection law in the European Union that governs the processing of personal data.
- **HIPAA (Health Insurance Portability and Accountability Act):** Protects the privacy and security of health information in the United States.
- **PCI DSS (Payment Card Industry Data Security Standard):** A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

Incident Response and Business Continuity

Despite best efforts, security incidents can still occur. Having well-defined incident response and business continuity plans is critical for minimizing damage and resuming operations quickly. These are fundamental topics for **cyber security fundamentals 2020 exam answers**.

Incident Response Plan (IRP)

An IRP is a documented set of procedures that outlines how an organization will respond to a security breach or cyberattack. A typical IRP includes:

- **Preparation:** Establishing policies, procedures, and tools for incident response.
- **Identification:** Detecting and confirming a security incident.
- **Containment:** Limiting the scope and impact of the incident.
- **Eradication:** Removing the threat from the environment.
- **Recovery:** Restoring affected systems and data to normal operations.
- **Lessons Learned:** Reviewing the incident and the response to improve future preparedness.

Business Continuity and Disaster Recovery (BCDR)

BCDR plans ensure that an organization can continue to operate during and after a disruptive event, whether it's a cyberattack, natural disaster, or system failure.

- **Business Continuity:** Focuses on maintaining essential business functions during a crisis.
- **Disaster Recovery:** Specifically deals with restoring IT infrastructure and data after a disruptive event.
- **Backup and Recovery Strategies:** Implementing regular data backups and testing recovery procedures.
- **Redundancy:** Building redundant systems and infrastructure to ensure availability.

Cryptography and Secure Communication

Cryptography is the backbone of secure communication and data protection. Understanding its principles is vital for anyone dealing with **cyber security fundamentals 2020 exam answers**.

Encryption Algorithms

Different algorithms offer varying levels of security and performance. Key concepts include:

- **AES (Advanced Encryption Standard):** A widely used symmetric encryption algorithm considered highly secure.

- **RSA:** A popular asymmetric encryption algorithm used for secure data transmission and digital signatures.
- **Diffie-Hellman Key Exchange:** A method for two parties to securely establish a shared secret key over an insecure channel.

Hashing Functions

Hashing is essential for data integrity and password security.

- **SHA-256 (Secure Hash Algorithm 256-bit):** A cryptographic hash function that produces a 256-bit hash value.
- **MD5 (Message-Digest Algorithm 5):** An older hashing algorithm, now considered cryptographically broken due to collision vulnerabilities.

Digital Signatures

Digital signatures use asymmetric cryptography to verify the authenticity and integrity of a digital document or message. They ensure non-repudiation, meaning the sender cannot later deny having sent the message.

Secure Communication Protocols

Protocols that use encryption to secure data in transit are critical.

- **TLS/SSL (Transport Layer Security/Secure Sockets Layer):** Protocols used to secure internet communications, commonly seen as HTTPS.
- **SSH (Secure Shell):** A network protocol used for secure remote login and other secure network services over an unsecured network.
- **VPN (Virtual Private Network):** Creates an encrypted tunnel over a public network to provide secure remote access and protect online privacy.

Network Security Fundamentals

Securing networks is a broad and essential area of cybersecurity. Understanding these fundamentals is a recurring theme in **cyber security fundamentals 2020 exam answers**.

Network Devices and Their Security

Different network devices play crucial roles and require specific security considerations.

- **Routers:** Direct traffic between networks. Secure configurations are vital to prevent unauthorized access and traffic manipulation.
- **Switches:** Connect devices within a local area network (LAN). VLANs (Virtual Local Area Networks) can segment traffic for better security.
- **Firewalls:** Act as a barrier between a trusted internal network and untrusted external networks. They filter incoming and outgoing traffic based on predefined security rules.
- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** IDS monitor network traffic for suspicious activity, while IPS can actively block or prevent detected threats.

Network Segmentation

Dividing a network into smaller, isolated segments (using VLANs, subnets, or firewalls) limits the lateral movement of attackers and contains the impact of a breach.

Wireless Security

Securing wireless networks is critical, as they are inherently more exposed than wired networks.

- **WPA3 (Wi-Fi Protected Access 3):** The latest standard for Wi-Fi security, offering improved encryption and protection.
- **SSID (Service Set Identifier) Hiding:** While not a strong security measure, hiding the SSID can deter casual observation.
- **MAC Address Filtering:** Allowing only devices with specific MAC addresses to connect, though this can be spoofed.

Network Security Best Practices

Implementing secure network configurations and protocols is paramount.

- Regularly update firewall rules and network device firmware.
- Enforce strong passwords and access controls for network devices.
- Monitor network traffic for anomalies and suspicious activity.
- Use VPNs for remote access.
- Segment networks to limit the blast radius of security incidents.

Application Security and Secure Coding

Ensuring that applications are developed and maintained with security in mind is crucial to prevent vulnerabilities. This area is increasingly important in **cyber security fundamentals 2020 exam answers**.

Common Application Vulnerabilities

Understanding common programming flaws that attackers exploit is key.

- **SQL Injection:** Attackers insert malicious SQL code into input fields to manipulate database queries.
- **Cross-Site Scripting (XSS):** Attackers inject malicious scripts into web pages viewed by other users.
- **Buffer Overflow:** Writing more data to a buffer than it can hold, potentially overwriting adjacent memory and executing malicious code.
- **Insecure Direct Object References (IDOR):** Exposing internal implementation objects by providing direct access to a key or parameter.
- **Security Misconfiguration:** Incorrectly configured security settings that leave systems vulnerable.

Secure Coding Practices

Developers should follow secure coding principles throughout the software development lifecycle (SDLC).

- Input validation and sanitization to prevent injection attacks.
- Parameterized queries for database interactions.
- Secure error handling to avoid revealing sensitive information.
- Proper authentication and authorization checks at all layers.
- Regular security testing, including static and dynamic analysis.

Web Application Firewalls (WAFs)

WAFs protect web applications by filtering, monitoring, and blocking HTTP traffic to and from a web application. They can help mitigate common web vulnerabilities.

Identity and Access Management (IAM)

IAM is critical for ensuring that the right individuals have the appropriate access to resources at the right times and for the right reasons. This is a foundational concept in **cyber security fundamentals 2020 exam answers**.

User Provisioning and Deprovisioning

The process of creating, managing, and deleting user accounts and their access rights is a key aspect of IAM. Offboarding employees promptly and revoking their access is crucial to prevent unauthorized access.

Authentication Methods

Beyond passwords, modern IAM relies on robust authentication.

- **Multi-Factor Authentication (MFA):** As mentioned earlier, MFA is a cornerstone of secure

access.

- **Single Sign-On (SSO):** Allows users to log in once and gain access to multiple applications, improving user experience and security if implemented correctly.
- **Federated Identity:** Enables users to use one set of login credentials to access multiple unrelated systems.

Authorization Models

How permissions are granted and managed is central to IAM.

- **Role-Based Access Control (RBAC):** Simplifies permission management by assigning access based on job functions.
- **Attribute-Based Access Control (ABAC):** Offers more granular control by defining policies based on attributes.

Privileged Access Management (PAM)

PAM solutions focus on managing and monitoring accounts with elevated privileges, such as administrators. This is critical as compromised privileged accounts can cause significant damage.

Physical Security in Cybersecurity

While much of cybersecurity focuses on digital threats, physical security is an equally important layer. Compromised physical access can negate even the strongest digital defenses, a point often considered in **cyber security fundamentals 2020 exam answers**.

Securing Data Centers and Server Rooms

These locations house critical IT infrastructure and must be protected from unauthorized physical access.

- Access controls (key cards, biometric scanners).

- Surveillance systems (CCTV).
- Visitor logs and escort policies.
- Secure racks and cabinets.

Device Security

Protecting physical endpoints is also vital.

- **Laptop locks:** To secure laptops in public spaces.
- **Screen privacy filters:** To prevent shoulder surfing.
- **Secure disposal of old hardware:** Ensuring data is destroyed before devices are discarded.

Environmental Controls

Protecting IT equipment from environmental hazards is part of physical security.

- Fire suppression systems.
- Temperature and humidity monitoring and control.
- Surge protectors and uninterruptible power supplies (UPS).

Cloud Security Fundamentals

The widespread adoption of cloud computing in 2020 and beyond made cloud security a paramount concern. Understanding cloud security models and best practices is essential for **cyber security fundamentals 2020 exam answers**.

Cloud Service Models

Understanding the shared responsibility model is crucial for cloud security.

- **IaaS (Infrastructure as a Service):** The cloud provider manages the underlying infrastructure, while the customer manages the operating system, applications, and data.
- **PaaS (Platform as a Service):** The provider manages the infrastructure and operating system, while the customer manages applications and data.
- **SaaS (Software as a Service):** The provider manages all aspects of the service, and the customer uses the application.

Shared Responsibility Model

In cloud computing, security is a shared responsibility between the cloud provider and the customer. The provider is responsible for the security of the cloud, while the customer is responsible for security in the cloud.

Cloud Security Controls

Key controls in the cloud environment include:

- Identity and Access Management (IAM) for cloud resources.
- Data encryption for data at rest and in transit.
- Network security configurations (e.g., virtual private clouds, security groups).
- Configuration management and vulnerability scanning of cloud assets.
- Logging and monitoring of cloud activity.

Container Security and Serverless Security

As cloud-native technologies like containers and serverless functions gained prominence, their specific security considerations became increasingly important.

Emerging Trends in Cybersecurity

The cybersecurity landscape is constantly evolving, and staying abreast of emerging trends is vital.

While focusing on **cyber security fundamentals 2020 exam answers**, it's also beneficial to look ahead.

Artificial Intelligence (AI) and Machine Learning (ML) in Cybersecurity

AI and ML are increasingly used for threat detection, anomaly detection, and automating security responses. They can analyze vast amounts of data to identify patterns indicative of malicious activity.

The Internet of Things (IoT) Security

The proliferation of IoT devices has created new attack surfaces. Many IoT devices have weak security, making them targets for botnets or entry points into networks.

Ransomware Evolution

Ransomware attacks have become more sophisticated, with attackers increasingly exfiltrating data before encrypting it (double extortion) and targeting critical infrastructure and supply chains.

Zero Trust Architecture

Zero Trust is a security framework that assumes no user or device, inside or outside the network, can be trusted by default. It requires strict verification for every access attempt.

Quantum Computing and Cryptography

While still largely in development, quantum computing has the potential to break current encryption methods. Research into quantum-resistant cryptography is ongoing.

Frequently Asked Questions

What is the primary purpose of the CIA triad in cybersecurity?

The CIA triad (Confidentiality, Integrity, and Availability) is a fundamental model in cybersecurity that outlines the core objectives for protecting information. Confidentiality ensures that data is only accessible to authorized individuals, Integrity guarantees that data is accurate and has not been tampered with, and Availability ensures that authorized users can access the information when they

need it.

Explain the concept of 'least privilege' and why it's important in cybersecurity.

The principle of 'least privilege' dictates that a user, program, or process should only have the minimum necessary permissions to perform its intended function. This limits the potential damage if an account is compromised or a program malfunctions, reducing the attack surface.

What are the key differences between symmetric and asymmetric encryption?

Symmetric encryption uses a single, shared secret key for both encryption and decryption, making it faster. Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption, enabling secure communication without pre-sharing a secret key.

Describe a common phishing attack and how users can protect themselves.

A phishing attack typically involves deceptive emails, messages, or websites designed to trick users into revealing sensitive information like passwords or credit card numbers. Users can protect themselves by being suspicious of unsolicited communications, verifying sender identities, avoiding clicking on suspicious links or attachments, and using strong, unique passwords.

What is malware and what are some common types?

Malware is malicious software designed to harm or exploit computer systems. Common types include viruses, worms, Trojans, ransomware, spyware, and adware.

Explain the purpose of a firewall in a network.

A firewall acts as a barrier between a trusted internal network and untrusted external networks (like the internet). It monitors and controls incoming and outgoing network traffic based on predetermined security rules, blocking unauthorized access and malicious traffic.

What is multi-factor authentication (MFA) and why is it recommended?

Multi-factor authentication (MFA) requires users to provide two or more different forms of verification before granting access to an account or system. This typically involves something the user knows (password), something the user has (a token or phone), and/or something the user is (biometrics). It significantly enhances security by making it much harder for unauthorized individuals to gain access.

What is the role of antivirus software in cybersecurity?

Antivirus software is designed to detect, prevent, and remove malicious software (malware) from computer systems. It scans files and programs for known malware signatures and uses heuristic

analysis to identify potentially malicious behavior.

Define 'social engineering' in the context of cybersecurity.

Social engineering is a psychological manipulation tactic used by attackers to trick individuals into divulging confidential information or performing actions that compromise security. It often exploits human trust, curiosity, or fear.

Additional Resources

Here are 9 book titles related to cybersecurity fundamentals, with a focus on concepts relevant to a 2020 exam, presented as requested:

1. *CompTIA Security+ SY0-501 Study Guide*
This comprehensive guide prepares individuals for the CompTIA Security+ certification exam, covering essential cybersecurity concepts. It delves into network security, threat management, cryptography, access control, and operational security. The book provides a structured approach to learning, ensuring a strong understanding of core security principles.

2. *Cybersecurity Fundamentals: An Introduction to Information Security*
This foundational text offers a broad overview of cybersecurity principles and practices. It explores the landscape of threats, vulnerabilities, and the importance of protecting digital assets. Key topics include risk management, security policies, and the basic building blocks of secure systems.

3. *The Practice of Network Security Monitoring: From Analysis to Action*
Focusing on practical application, this book guides readers through the process of detecting and responding to network security incidents. It covers essential techniques for network traffic analysis, log management, and identifying malicious activities. The content is vital for understanding how to monitor and secure network environments effectively.

4. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*
This classic text provides an in-depth exploration of cryptographic principles and their practical implementation. It details various algorithms, protocols, and the underlying mathematics that secure communications and data. Understanding cryptography is fundamental to many cybersecurity concepts tested in exams.

5. *CISSP All-in-One Exam Guide*
While targeting a more advanced certification, this guide covers a vast array of cybersecurity domains, many of which are fundamental. It systematically breaks down security and risk management, asset security, security architecture and engineering, and more. This book offers a deep dive into the breadth of cybersecurity knowledge.

6. *Malware Analyst's Cookbook: Defending Against Digital Attack*
This practical resource equips readers with the skills to analyze and understand malware. It provides step-by-step instructions and recipes for dissecting malicious software and identifying its behavior. A strong understanding of malware is crucial for comprehending modern cyber threats.

7. *Information Security Governance: A Practical Guide to Management*
This book emphasizes the management and governance aspects of information security. It outlines

strategies for creating and implementing effective security policies, procedures, and controls. The focus on organizational security and compliance is essential for a well-rounded understanding.

8. *OWASP Top 10 Security Risks: A Comprehensive Guide*
This title directly addresses the most critical web application security risks as identified by the Open Web Application Security Project. It explains each vulnerability in detail, along with methods for prevention and mitigation. Knowledge of these common web threats is a core component of many cybersecurity exams.

9. *The Hacker Playbook 3: Practical Guide To Penetration Testing*
This book provides a hands-on approach to penetration testing, simulating real-world attack scenarios. It details methodologies for identifying vulnerabilities and exploiting them, offering valuable insights into defensive strategies. Understanding the attacker's perspective is key to building robust defenses.

Cyber Security Fundamentals 2020 Exam Answers

Cyber Security Fundamentals 2020 Exam Answers

Related Articles

- cut and paste worksheets for 2nd grade
- couples therapy for trust issues
- covered wagons heading west painting rhetorical analysis

Back to Home