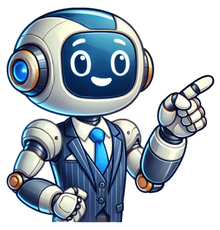
Continue



Cisco final exam answers introduction to cybersecurity

Cybersecurity is an ongoing effort to protect Internet-connected systems and the data associated with those systems from unauthorized use or harm. It's not about developing firewall technologies, but rather ensuring the integrity of these systems. Two objectives of ensuring data integrity are: Data is unaltered during transit and Data is not changed by unauthorized entities. The requirement of information security addressed through configuring access settings to require user authentication is confidentiality. By implementing a plan to add more web servers for load balancing and redundancy, the company is addressing scalability and availability. An employee's illegal actions as a company representative would put the company at legal risk. The answer is True. Cyberwarfare aims to gain advantage over adversaries by simulating possible war scenarios among nations. The difference between a virus and a worm is that a virus replicates itself by attaching to another file, whereas a worm can replicate itself independently. A type of attack that uses zombies is DDoS (Distributed Denial of Service). An abnormally high number of web page requests from different locations simultaneously is a sign of a DDoS attack. The best approach to prevent a compromised IoT device from maliciously accessing data and devices on a local network is to Place all IoT devices that have access to the Internet on an isolated network. To avoid getting spyware, it's best to Install software only from trusted websites and Install the latest operating system updates. Two security implementations that use biometrics are voice recognition and fingerprint. What information would put the privacy of patients at risk if included in an email sent by a medical office employee? First and last name, patient records, contact information, and next appointment details could compromise patient privacy. Two tools used for incident detection that can detect anomalous behavior, command and control traffic, and infected hosts are intrusion detection system (IDS) and Honeypot. A network administrator would use Nmap tool to detect and identify open ports, protect private IP addresses of internal hosts, identify specific network anomalies, collect and analyze security alerts and logs. The reconnaissance stage in the kill chain focuses on identifying and selecting targets. An example of a Cyber Kill Chain is a planned process of cyberattack that involves a series of worms based on the same core code. A honeypot tool is used to lure an attacker so that an administrator can capture, log, and analyze the behavior of the attack. The main function of the Cisco Security Incident Response Team is to ensure company, system, and data preservation. An IDS will take action upon detection of malicious traffic by creating a network alert and logging the detection, or rerouting malicious traffic to a honeypot. data encryption, identity proofing, and two-factor authentication measures are essential for ensuring confidentiality and integrity. Ensuring data integrity aims to prevent unauthorized changes or alterations during transmission, storage, or processing. This involves verifying the authenticity of data and maintaining its original form. To address scalability issues with a main web server, implementing load balancing and redundancy by adding more servers addresses availability requirements, ensuring the system can handle increased traffic and remain operational. Examples of cracking an encrypted password include brute-force attacks, rainbow tables, spraying dictionary attacks, and social engineering. Improper physical access management to resources can lead to weaknesses in security practices, race conditions, or buffer overflow vulnerabilities. Patient records containing confidential information should be transmitted securely to maintain privacy. To avoid getting spyware on a machine, it's essential to install the latest antivirus updates, install software from trusted websites, and keep operating system updates current. Before connecting to a public Wi-Fi network, ensure that your device isn't configured for file and media sharing, requires user authentication with encryption, and has a master password set for secure storage of passwords. The Cisco Security Incident Response Team's primary function is to provide incident response services to preserve company, system, and data integrity in the event of a security breach. Firewalls placed in front of web services include reverse proxy servers, which protect, hide, offload, and distribute access to web servers by filtering incoming traffic based on specific rules or policies. These measures are critical components of an effective information security strategy, enabling organizations to maintain confidentiality, integrity, and availability while protecting against various types of threats and vulnerabilities. The following certifications meet the U.S. Department of Defense Directive 8570.01-M requirements for IT security in the federal government: - EC Council Certified Ethical Hacker - Microsoft Technology Associate Security Fundamentals - ISACA CSX Cybersecurity Fundamentals - CompTIA Security+ - ISC2 Certified Information Systems Security Professional - Palo Alto Networks Certified Cybersecurity Associate These certifications are entry-level and meet the requirements for working in IT security for the federal government. The behavior of lending a colleague's identification badge is considered unethical as it may be a breach of company policies and protocols regarding personal identification badges. The certification that tests understanding and knowledge of looking for weaknesses and vulnerabilities using the same tools as malicious hackers but in a lawful manner is the Palo Alto Networks Certified Cybersecurity Associate or ISC2 Certified Information Systems Security Professional. Cyberwarfare's main purpose is to gain an advantage over adversaries, whether it be nations or competitors. A vulnerability that occurs when output depends on ordered or timed outputs is a race condition. The vulnerabilities discovered by Google security researchers are Shell shock and Spectre, which affect almost all CPUs released since 1995. Creating own security algorithms may introduce buffer overflow, race conditions, weaknesses in security practices, non-validated input, and access control problems. 1. Third-party applications should use secure methods to protect their users' passwords without exposing them. 2. Fingerprint, Phone, and Voice recognition are examples of biometric security implementations. 3. Application layer firewalls filter web content requests such as URLs and domain names. 4. A port scan that returns a 'dropped' response means that there was no reply from the host. 5. This employee's behavior is unethical because they are sharing confidential information with their new organization without permission. 6. CompTIA Security+, Microsoft Technology Associate Security Fundamentals, and EC Council Certified Ethical Hacker are examples of entry-level certifications for newcomers in cybersecurity. 7. True - Cybersecurity certifications can verify skills and knowledge and boost careers. 8. A virus focuses on gaining privileged access to a device, whereas a worm does not; a virus replicates itself by attaching to another file, whereas a worm can replicate independently; a virus can be used to launch DoS attacks but not DDoS, whereas a worm can be used for both. 9. This employee's behavior is unethical because they are sharing confidential information with their new organization without permission. 10. Context-aware application firewalls filter traffic based on user, device, role, application type and threat profile Blockchain technology records transactions in a decentralized, electronic ledger or blockchain system, providing anonymity and self-management with minimal interference from third parties. The states of data include Storage (data at rest), Transmission (data in transit), and Processing (data in process). False: Internet-based cameras and gaming gear can be subject to security breaches. Buffer overflow occurs when data is written beyond the memory areas allocated to an application, causing a vulnerability. An organization's IT department reports that their web server is receiving an abnormally high number of web page requests from different locations simultaneously, indicating a DDoS (Distributed Denial-of-Service) attack. Two commonly used port scanning applications are Network Mapper (Nmap) and Zenmap. Upon detection of malicious traffic, an IDS will create a network alert and log the detection to prevent further harm. Cybersecurity refers to the ongoing effort to protect Internet-connected systems and data from unauthorized use or harm. True: Educating employees, partners, and customers on how to prevent future breaches is crucial after a data breach. Ethical behavior: An employee pointing out a design flaw in a new product to the department manager demonstrates responsible and honest conduct. This statement describes Non-validated input as a security vulnerability, which occurs when data coming into a program has malicious content, designed to force the program to behave in an unintended way. Given text about cybersecurity questions seems mostly unrelated but let's focus on question 44 which asks about what port scan responses mean. A port scan is used to determine active ports on a host, and the response 'closed' means there was no reply from the host, implying that no service or application is listening on that specific port. This can indicate that the port is not in use or that it's being blocked by a firewall. 57. False - A data breach can severely damage an organization's reputation and trust with customers. 58. CompTIA Security+ - This certification targets high school and early college students, as well as anyone interested in a career change. 60. Firewalls Guards Technology Awareness, training and education Policy and procedure Camera - These are categories of security measures or controls. 62. To detect and identify open ports - A network administrator uses the Nmap tool for this purpose. 64. DDoS (Distributed Denial of Service) - This type of attack uses zombies to overload a system with traffic, similar to a DoS attack but originating from multiple sources. 66. Host-based firewall - This filters ports and system service calls on a single computer operating system. 67. DDoS (Distributed Denial of Service) - This attack disrupts services by overwhelming network devices with bogus traffic. 69. Several @Apollo employees reported slow network access, which led the administrator to investigate. 70. The investigation revealed that one employee's computer was infected with malware, causing the network slowdown. 71. To address this issue, the IT department will update the company's security software and educate employees on cybersecurity best practices. 72. Additionally, they will implement a monitoring system to quickly detect future issues before they become major problems. A third-party scanning program was downloaded for the printer, and the network performance has been slow. Worms are a type of malware that can cause slow network performance. They replicate independently using vulnerabilities in networks and do not require user participation after initial infection. The cyber kill chain is a planned process of cyber attack. Business continuity and disaster recovery refer to strategies for minimizing downtime, but they don't directly address risk management. An employee who was laid off and then hired by another organization within a week may be sharing confidential information, which raises ethical concerns. Reconnaissance is the first stage of the kill chain where attackers identify and select targets. A company can be held legally responsible if an employee's actions are deemed illegal while acting as a representative of the company. Google Chrome has several private browser modes, including Private tab, InPrivate, and Incognito. MITMO attacks involve capturing two-step verification SMS messages to steal user credentials. Configuring access settings that require authentication before accessing certain web pages addresses confidentiality by ensuring data is accessed only by authorized individuals.