SolveMyQues
Test your skills online

Sample Questions with Answers

Cybersecurity - Ethical Hacking

Generated on May 28, 2026 at 6:13 PM

Cybersecurity

[NOTE] Important Note: This PDF contains sample questions with complete answers and explanations. **Visit SolveMyQues.com** for our complete question bank, interactive tests, and detailed performance tracking!

Question 1:

What is cybersecurity and why is it important?

[ANSWER] Answer & Explanation:

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage.\n\n**What cybersecurity protects:**\n• **Confidentiality** - Ensuring data is only accessible to authorized users\n• **Integrity** - Maintaining accuracy and completeness of data\n• **Availability** - Ensuring systems and data are accessible when needed\n\n**Why cybersecurity is critical:**\n• **Financial protection** - Prevents costly data breaches and ransomware\n• **Privacy protection** - Safeguards personal and sensitive information\n• **Business continuity** - Maintains operations and prevents downtime\n• **Regulatory compliance** - Meets legal requirements (GDPR, HIPAA, SOX)\n• **Reputation management** - Protects brand trust and customer confidence\n\n**Common threats addressed:**\n• Malware (viruses, ransomware, trojans)\n• Phishing and social engineering attacks\n• Data breaches and identity theft\n• Denial of Service (DoS) attacks\n• Insider threats and human error\n\n**Real-world impact:**\nCyberattacks cost businesses an average of $4.45 million per breach (2023). Major incidents like Equifax (147M records), Target (40M+ cards), and Colonial Pipeline (infrastructure shutdown) demonstrate the devastating consequences of inadequate cybersecurity.\n\n**Best practices:**\n• Implement defense-in-depth strategy\n• Regular security awareness training\n• Keep systems updated and patched\n• Use strong authentication methods\n• Monitor and respond to threats continuously

Question 2:

What are the different types of malware and how do they work?

[ANSWER] Answer & Explanation:

Malware (malicious software) is designed to damage, disrupt, or gain unauthorized access to computer systems.\n\n**Major malware types:**\n\n**1. Viruses:**\n• **How they work** - Attach to legitimate files and replicate when executed\n• **Spread method** - Through infected files, email attachments, removable media\n• **Example** - ILOVEYOU virus (2000) infected 50M+ computers via email\n\n**2. Worms:**\n• **How they work** - Self-replicating programs that spread across networks\n• **Spread method** - Exploit network vulnerabilities without user interaction\n• **Example** - WannaCry ransomware worm (2017) affected 300k+ computers\n\n**3. Trojans:**\n• **How they work** - Disguise as legitimate software to trick users\n• **Purpose** - Create backdoors, steal data, or download additional malware\n• **Example** - Banking trojans that steal financial credentials\n\n**4. Ransomware:**\n• **How they work** - Encrypt files and demand payment for decryption key\n• **Impact** - Can paralyze entire organizations and critical infrastructure\n• **Example** - Colonial Pipeline attack (2021) disrupted US fuel supply\n\n**5. Spyware:**\n• **How they work** - Secretly monitor and collect user information\n• **Data stolen** - Passwords, browsing habits, personal information\n• **Example** - Keyloggers that record keystrokes\n\n**6. Adware:**\n• **How they work** - Display unwanted advertisements and track behavior\n• **Impact** - Slows system performance and compromises privacy\n\n**Protection strategies:**\n• Use reputable antivirus software\n• Keep systems and software updated\n• Avoid suspicious downloads and email attachments\n• Regular system backups\n• Network segmentation and access controls

Question 3:

What is the difference between authentication and authorization?

[ANSWER] Answer & Explanation:

Authentication and authorization are fundamental security concepts that work together to control system access.\n\n**Authentication - "Who are you?"**\n• **Purpose** - Verifies the identity of a user or system\n• **Process** - User provides credentials to prove their identity\n• **Methods** - Username/password, biometrics, smart cards, tokens\n• **Example** - Entering your username and password to log into email\n\n**Authorization - "What can you do?"**\n• **Purpose** - Determines what resources an authenticated user can access\n• **Process** - System checks user permissions against requested resources\n• **Methods** - Role-based access control (RBAC), access control lists (ACLs)\n• **Example** - Admin can delete files, regular user can only read them\n\n**Key differences:**\n\n| Aspect | Authentication | Authorization |\n|--------|---------------|---------------|\n| **Question** | Who are you? | What can you access? |\n| **When** | First step | After authentication |\n| **Verifies** | Identity | Permissions |\n| **Methods** | Passwords, biometrics | Roles, policies |\n| **Failure** | Access denied | Limited access |\n\n**Real-world example:**\n1. **Authentication** - Employee badges into office building (proves identity)\n2. **Authorization** - Badge allows access to specific floors/rooms (defines permissions)\n\n**Multi-factor authentication (MFA):**\nCombines multiple authentication factors:\n• **Something you know** - Password, PIN\n• **Something you have** - Phone, token, smart card\n• **Something you are** - Fingerprint, face recognition\n\n**Best practices:**\n• Implement strong authentication (MFA)\n• Follow principle of least privilege\n• Regular access reviews and updates\n• Separate admin and user accounts\n• Monitor and log access attempts

Question 4:

What is a firewall and how does it protect networks?

[ANSWER] Answer & Explanation:

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.\n\n**How firewalls work:**\n• **Traffic filtering** - Examines data packets and applies security rules\n• **Access control** - Allows or blocks traffic based on source, destination, port\n• **Network barrier** - Creates a protective boundary between trusted and untrusted networks\n• **Logging** - Records traffic patterns and security events for analysis\n\n**Types of firewalls:**\n\n**1. Packet filtering (Stateless):**\n• **Function** - Examines individual packets against static rules\n• **Criteria** - Source/destination IP, port numbers, protocol type\n• **Pros** - Fast processing, low resource usage\n• **Cons** - Cannot track connection state, limited security\n\n**2. Stateful inspection:**\n• **Function** - Tracks connection state and context\n• **Intelligence** - Remembers previous packets in the connection\n• **Security** - Better protection against sophisticated attacks\n• **Example** - Allows return traffic for established connections\n\n**3. Application layer (Proxy):**\n• **Function** - Inspects application-specific data and protocols\n• **Deep inspection** - Understands HTTP, FTP, SMTP content\n• **Security** - Highest level of protection and control\n• **Performance** - Slower due to detailed analysis\n\n**4. Next-generation firewalls (NGFW):**\n• **Features** - Combines traditional firewall with IPS, application awareness\n• **Intelligence** - User identity, application control, threat intelligence\n• **Integration** - Works with security information and event management (SIEM)\n\n**Firewall deployment:**\n• **Network perimeter** - Between internal network and internet\n• **Internal segmentation** - Between network zones (DMZ, servers, workstations)\n• **Host-based** - Software firewall on individual devices\n\n**Best practices:**\n• Default deny policy (block all, allow specific)\n• Regular rule review and cleanup\n• Monitor firewall logs for threats\n• Keep firmware updated\n• Test firewall rules and configurations

Question 5:

What is phishing and how can organizations protect against it?

[ANSWER] Answer & Explanation:

Phishing is a social engineering attack where cybercriminals impersonate legitimate entities to steal sensitive information like passwords, credit card numbers, or personal data.\n\n**How phishing works:**\n• **Deception** - Attackers create fake emails, websites, or messages\n• **Urgency** - Create false sense of urgency to bypass critical thinking\n• **Credential harvesting** - Trick users into entering sensitive information\n• **Malware delivery** - Distribute malicious attachments or links\n\n**Common phishing types:**\n\n**1. Email phishing:**\n• **Method** - Mass emails impersonating banks, services, or colleagues\n• **Example** - "Your account will be suspended, click here to verify"\n• **Indicators** - Generic greetings, urgent language, suspicious links\n\n**2. Spear phishing:**\n• **Method** - Targeted attacks using personal information\n• **Research** - Attackers study victims through social media, company websites\n• **Example** - CEO impersonation requesting urgent wire transfer\n\n**3. Whaling:**\n• **Target** - High-profile executives and decision makers\n• **Impact** - Access to sensitive corporate information and systems\n• **Sophistication** - Highly personalized and convincing attacks\n\n**4. Smishing (SMS phishing):**\n• **Method** - Text messages with malicious links or requests\n• **Example** - "Package delivery failed, click to reschedule"\n\n**5. Vishing (Voice phishing):**\n• **Method** - Phone calls impersonating legitimate organizations\n• **Example** - Fake tech support requesting remote access\n\n**Protection strategies:**\n\n**Technical controls:**\n• Email security gateways with anti-phishing filters\n• Web filtering to block malicious websites\n• Multi-factor authentication (MFA)\n• Email authentication (SPF, DKIM, DMARC)\n\n**User education:**\n• Regular security awareness training\n• Simulated phishing exercises\n• Clear reporting procedures for suspicious emails\n• Verification protocols for sensitive requests\n\n**Best practices:**\n• Verify sender identity through separate communication channel\n• Hover over links to check actual destination\n• Be suspicious of urgent or threatening language\n• Never provide sensitive information via email or phone\n• Keep software and browsers updated

[FEATURES] Want More Questions & Features?

Visit SolveMyQues.com for:

- [+] Complete question bank with detailed answers & explanations
- [+] Interactive skill assessment tests with instant results
- [+] Performance tracking and personalized recommendations
- [+] Achievement certificates and progress reports
- [+] Expert explanations and step-by-step solutions
- [+] Ask questions to our expert team
- [+] Daily challenges and leaderboards

[WEB] Website: www.solvemyques.com

[EMAIL] Email: support@solvemyques.com