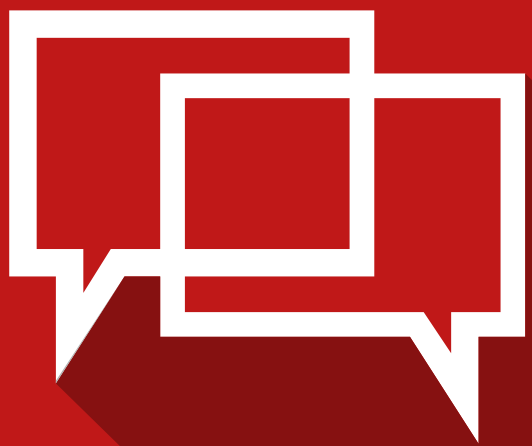
200 IT Security Job Interview Questions

The Questions IT Leaders Ask



McAfee™
Together is power.

IT security professionals with the right skills are in high demand. In 2015, the unemployment rate for information security managers averaged 0.9%, which is as close to full employment as you can get. However, one of the things hiring managers still complain about is a lack of skilled IT professionals, as evidenced by the frustration CISOs and others express after interviewing candidates.

Below is a list of interview questions categorized by different cybersecurity job roles intended to reveal a candidate's strengths and most glaring weaknesses. Categories include:

- General IT Security Administration
- Network Security
- Application Security
- Security Architect
- Risk Management
- Security Audit, Testing and Incident Response
- Cryptography

The questions evaluate a broad range of candidate's technical skills, understanding of cybersecurity terminology and technology as well as their ability to think and solve problems.

1. What is information security and how is it achieved?
2. What are the core principles of information security?
3. What is non-repudiation (as it applies to IT security)?
4. What is the relationship between information security and data availability?
5. What is a security policy and why do we need one?
6. What is the difference between logical and physical security? Can you give an example of both?
7. What's an acceptable level of risk?
8. What are the most common types of attacks that threaten enterprise data security?
9. What is the difference between a threat and a vulnerability?
10. Can you give me an example of common security vulnerabilities?
11. Are you familiar with any security management frameworks such as ISO/IEC 27002?
12. What is a security control?
13. What are the different types of security control?
14. Can you describe the information lifecycle? How do you ensure information security at each phase?
15. What is Information Security Governance?
16. What are your professional values? Why are professional ethics important in the information security field?
17. Are open-source projects more or less secure than proprietary ones?
18. Who do you look up to within the field of Information Security? Why?
19. Where do you get your security news from?
20. What's the difference between symmetric and public-key cryptography?
21. What kind of network do you have at home?
22. What are the advantages offered by bug bounty programs over normal testing practices?
23. What are your first three steps when securing a Linux server?
24. What are your first three steps when securing a Windows server?
25. Who's more dangerous to an organization, insiders or outsiders?
26. Why is DNS monitoring important?
27. How would traceroute help you find out where a breakdown in communication is?
28. Why would you want to use SSH from a Windows PC?
29. How would you find out what a POST code means?
30. What is the difference between a black hat and a white hat?
31. What do you think of social networking sites such as Facebook and LinkedIn?
32. Why are internal threats often more successful than external threats?

33. Why is deleted data not truly gone when you delete it?
34. What is the Chain of Custody?
35. How would you permanently remove the threat of data falling into the wrong hands?
36. What is exfiltration?
37. How do you protect your home wireless access point?
38. If you were going to break into a database-based website, how would you do it?
39. What is the CIA triangle?
40. What is the difference between information protection and information assurance?
41. How would you lock down a mobile device?
42. What is the difference between closed-source and open-source? Which is better?
43. What is your opinion on hacktivist groups such as Anonymous?

Network security

44. What port does ping work over?
45. Do you prefer filtered ports or closed ports on your firewall?
46. How exactly does traceroute/tracert work at the protocol level?
47. What are Linux's strengths and weaknesses vs. Windows?
48. What is a firewall? And provide an example of how a firewall can be bypassed by an outsider to access the corporate network.
49. Besides firewalls, what other devices are used to enforce network boundaries?
50. What is the role of network boundaries in information security?
51. What does an intrusion detection system do? How does it do it?
52. What is a honeypot? What type of attack does it defend against?
53. What technologies and approaches are used to secure information and services deployed on cloud computing infrastructure?
54. What information security challenges are faced in a cloud computing environment?
55. Can you give me an overview of IP multicast?
56. How many bits do you need for a subnet size?
57. What is packet filtering?
58. Can you explain the difference between a packet filtering firewall and an application layer firewall?
59. What are the layers of the OSI model?
60. How would you login to Active Directory from a Linux or Mac box?
61. What is an easy way to configure a network to allow only a single computer to login on a particular jack?
62. What are the three ways to authenticate a person?
63. You find out that there is an active problem on your network. You can fix it, but it is out of your jurisdiction. What do you do?
64. How would you compromise an "office workstation" at a hotel?
65. What is worse in firewall detection, a false negative or a false positive? And why?
66. How would you judge if a remote server is running IIS or Apache?
67. What is the difference between an HIDS and a NIDS?

Application security

68. Describe the last program or script that you wrote. What problem did it solve?
69. Can you briefly discuss the role of information security in each phase of the software development lifecycle?
70. How would you implement a secure login field on a high traffic website where performance is a consideration?
71. What are the various ways to handle account brute forcing?
72. What is cross-site request forgery?

73. How does one defend against CSRF?
74. If you were a site administrator looking for incoming CSRF attacks, what would you look for?
75. What's the difference between HTTP and HTML?
76. How does HTTP handle state?
77. What exactly is cross-site scripting?
78. What's the difference between stored and reflected XSS?
79. What are the common defenses against XSS?
80. You are remoted in to a headless system in a remote area. You have no physical access to the hardware and you need to perform an OS installation. What do you do?
81. On a Windows network, why is it easier to break into a local account than an AD account?

Security architect

82. Explain data leakage and give examples of some of the root causes.
83. What are some effective ways to control data leakage?
84. Describe the 80/20 rules of networking.
85. What are web server vulnerabilities and name a few methods to prevent web server attacks?
86. What are the most damaging types of malwares?
87. What's your preferred method of giving remote employees access to the company network and are there any weaknesses associated to it?
88. List a couple of tests that you would do to a network to identify security flaws.
89. What kind of websites and cloud services would you block?
90. What type of security flaw is there in VPN?
91. What is a DDoS attack?
92. Can you describe the role of security operations in the enterprise?
93. What is layered security architecture? Is it a good approach? Why?
94. Have you designed security measures that span overlapping information domains? Can you give me a brief overview of the solution?
95. How do you ensure that a design anticipates human error?
96. How do you ensure that a design achieves regulatory compliance?
97. What is capability-based security? Have you incorporated this pattern into your designs? How?
98. Can you give me a few examples of security architecture requirements?
99. Who typically owns security architecture requirements and what stakeholders contribute?
100. What special security challenges does SOA present?
101. What security challenges do unified communications present?
102. Do you take a different approach to security architecture for a COTS vs a custom solution?
103. Have you architected a security solution that involved SaaS components? What challenges did you face?
104. Have you worked on a project in which stakeholders choose to accept identified security risks that worried you? How did you handle the situation?
105. You see a user logging in as root to perform basic functions. Is this a problem?
106. What is data protection in transit vs data protection at rest?
107. You need to reset a password-protected BIOS configuration. What do you do?

Risk management

108. Is there an acceptable level of risk?
109. How do you measure risk? Can you give an example of a specific metric that measures information security risk?
110. Can you give me an example of risk trade-offs (e.g. risk vs cost)?
111. What is incident management?
112. What is business continuity management? How does it relate to security?
113. What is the primary reason most companies haven't fixed their vulnerabilities?

114. What's the goal of information security within an organization?
115. What's the difference between a threat, vulnerability, and a risk?
116. If you were to start a job as head engineer or CSO at a Fortune 500 company due to the previous guy being fired for incompetence, what would your priorities be? [Imagine you start on day one with no knowledge of the environment]
117. As a corporate information security professional, what's more important to focus on: threats or vulnerabilities?
118. If I'm on my laptop, here inside my company, and I have just plugged in my network cable. How many packets must leave my NIC in order to complete a traceroute to twitter.com?
119. How would you build the ultimate botnet?
120. What are the primary design flaws in HTTP, and how would you improve it?
121. If you could re-design TCP, what would you fix?
122. What is the one feature you would add to DNS to improve it the most?
123. What is likely to be the primary protocol used for the Internet of Things in 10 years?
124. If you had to get rid of a layer of the OSI model, which would it be?
125. What is residual risk?
126. What is the difference between a vulnerability and an exploit?

Security audits, testing & incident response

127. What is an IT security audit?
128. What is an RFC?
129. What type of systems should be audited?
130. Have you worked in a virtualized environment?
131. What is the most difficult part of auditing for you?
132. Describe the most difficult auditing procedure you've implemented.
133. What is change management?
134. What types of RFC or change management software have you used?
135. What do you do if a rollout goes wrong?
136. How do you manage system major incidents?
137. How do you ask developers to document changes?
138. How do you compare files that might have changed since the last time you looked at them?
139. Name a few types of security breaches.
140. What is a common method of disrupting enterprise systems?
141. What are some security software tools you can use to monitor the network?
142. What should you do after you suspect a network has been hacked?
143. How can you encrypt email to secure transmissions about the company?
144. What document describes steps to bring up a network that's had a major outage?
145. How can you ensure backups are secure?
146. What is one way to do a cross-script hack?
147. How can you avoid cross script hacks?
148. How do you test information security?
149. What is the difference between black box and white box penetration testing?
150. What is a vulnerability scan?
151. In pen testing what's better, a red team or a blue team?
152. Why would you bring in an outside contractor to perform a penetration test?

Cryptography

153. What is secret-key cryptography?
154. What is public-key cryptography?
155. What is a session key?
156. What is RSA?

157. How fast is RSA?
158. What would it take to break RSA?
159. Are strong primes necessary for RSA?
160. How large a module (key) should be used in RSA?
161. How large should the primes be?
162. How is RSA used for authentication in practice? What are RSA digital signatures?
163. What are the alternatives to RSA?
164. Is RSA currently in use today?
165. What are DSS and DSA?
166. What is difference between DSA and RSA?
167. Is DSA secure?
168. What are special signature schemes?
169. What is a blind signature scheme?
170. What is a designated confirmer signatures?
171. What is a fail-stop signature scheme?
172. What is a group signature?
173. What is blowfish?
174. What is SAFER?
175. What is FEAL?
176. What is Shipjack?
177. What is stream cipher?
178. What is the advantage of public-key cryptography over secret-key cryptography?
179. What is the advantage of secret-key cryptography over public-key cryptography?
180. What is Message Authentication Code (MAC)?
181. What is a block cipher?
182. What are different block cipher modes of operation?
183. What is a stream cipher? Name a most widely used stream cipher.
184. What is one-way hash function?
185. What is collision when we talk about hash functions?
186. What are the applications of a hash function?
187. What is trapdoor function?
188. Cryptographically speaking, what is the main method of building a shared secret over a public medium?
189. What's the difference between Diffie-Hellman and RSA?
190. What kind of attack is a standard Diffie-Hellman exchange vulnerable to?
191. What's the difference between encoding, encryption, and hashing?
192. In public-key cryptography you have a public and a private key, and you often perform both encryption and signing functions. Which key is used for which function?
193. What's the difference between Symmetric and Asymmetric encryption?
194. If you had to both encrypt and compress data during transmission, which would you do first, and why?
195. What is SSL and why is it not enough when it comes to encryption?
196. What is salting, and why is it used?
197. What are salted hashes?
198. What is the Three-way handshake? How can it be used to create a DOS attack?
199. What's more secure, SSL or HTTPS?
200. Can you describe rainbow tables?