Here are the 300 interview questions for cyber security roles

Generic

1. Can you name some of the emerging cyber threats?
2. Can you walk me through economics of cyber security?
3. What parts of the information security should the organisations outsource?
4. What security conferences have you participated over the past 24 months?
5. Can you explain some ways cyber criminals are using services like LinkedIn?
6. Can you name a few leading cyber security vendors? What do they do?
7. What is information security and how is it achieved?
8. What are the core principles of information security?
9. What is non-repudiation (as it applies to IT security)?
10. As a CISO how would you justify a security spent to the board of directors?
11. How often should the information security be covered in the boardroom, why?
12. What is the relationship between information security and data availability?
13. What is a security policy and why do we need one?
14. What is the difference between logical and physical security? Can you give an example of both?
15. What's an acceptable level of risk?
16. How does Gartner rank the vendors in their Magic Quadrant?
17. What are the most common types of attacks that threaten enterprise data security?
18. What is the difference between a threat and a vulnerability?
19. Can you give me an example of common security vulnerabilities?
20. Are you familiar with any security management frameworks such as ISO/IEC 27002?
21. What is a security control?
22. What are the different types of security control?
23. Can you describe the information lifecycle? How do you ensure information security at each phase?
24. What is Information Security Governance?
25. What are your professional values? Why are professional ethics important in the information security field?
26. Is geo-blocking a valid security control?
27. Are open-source projects more or less secure than proprietary ones?
28. Who do you look up to within the field of Information Security? Why?
29. Where do you get your security news from?
30. What's the difference between symmetric and public-key cryptography?
31. What kind of network do you have at home?
32. What are the advantages offered by bug bounty programs over normal testing practices?
33. What are your first three steps when securing a Linux server?
34. What are your first three steps when securing a Windows server?
35. What are your first three steps when securing a web application?
36. What are the security risks of IoT devices?
37. Who's more dangerous to an organization, insiders or outsiders?
38. Why is DNS monitoring important?

39. How would traceroute help you find out where a breakdown in communication is?
40. Why would you want to use SSH from a Windows PC?
41. How would you find out what a POST code means?
42. What is the difference between a black hat and a white hat?
43. What do you think of social networking sites such as Facebook and LinkedIn?
44. Why are internal threats often more successful than external threats?
45. Why is deleted data not truly gone when you delete it?
46. What is the Chain of Custody?
47. How would you permanently remove the threat of data falling into the wrong hands?
48. What is exfiltration?
49. How do you protect your home wireless access point?
50. If you were going to break into a database-based website, how would you do it?
51. What is the CIA triangle?
52. What is the difference between information protection and information assurance?
53. How would you lock down a mobile device?
54. How can you check are the mobile application on your phone secure to use?
55. Which is more secure Android or iOS, why?
56. What is the difference between closed-source and open-source? Which is better?
57. What is your opinion on hacktivist groups such as Anonymous?
58. How would you explain the threat of deep fakes?
59. Which one is more secure, a strong password or biometric authentication?
60. What's the difference between deep web and dark web?
61. Why ransomware doesn't affect the mobile devices?
62. What is MITRE ATTACK?
63. Should CISO report to CIO or CEO and why is that?
64. What is pineapple device?
65. What is Raspberry Pie?
66. What is Kubernetes?
67. What role does the AI and machine learning have in information security?
68. What application would you use to securely communicate between mobile devices?
69. What does proxy do?
70. Can you explain man-in-the middle attack?
71. What is the most secure authentication methodology, why?
72. Why the IT and security teams don't like agents?
73. Can you name a few recent security breaches?
74. What is GDPR and does it affect you?
75. What role does the automation have in information security?
76. What is the difference between SIEM and UEBA?
77. Can give me an example of supply chain attack?
78. Can you define what is APT?
79. Why are the insurance companies paying out the ransomware demands?
80. What are the top 3 countries in information war?
81. Can you explain some ways the attackers are using AI?
82. Why are the cyber insurance premiums raising?

Cloud security

83. Why are so many S3 Bucket's breached?
84. What does the shared responsibility model in cloud mean?
85. What is the advantage of API over forward proxy?
86. How would you secure the East-West traffic in the cloud?
87. How would you secure the traffic between cloud services?
88. Who is responsible for securing the data and users when using SaaS or IaaS services?
89. Why are the containers vulnerable?
90. What are some of the security risks for the organisation when using Slack or Microsoft Teams?
91. Why does it take so long for organisations to move their workloads to the cloud?
92. Can you name the advantages of cloud-based databases?
93. Can you name a few security software tools that can help you monitor cloud environments?
94. What are things to take into consideration when using public cloud instead of private?
95. What is CASB?

Network security

96. What port does ping work over?
97. Do you prefer filtered ports or closed ports on your firewall?
98. How exactly does traceroute/tracert work at the protocol level?
99. What are Linux's strengths and weaknesses vs. Windows?
100. What is a firewall? And provide an example of how a firewall can be bypassed by an outsider to access the corporate network.
101. Besides firewalls, what other devices are used to enforce network boundaries?
102. What is the role of network boundaries in information security?
103. What does an intrusion detection system do? How does it do it?
104. What is a honeypot? What type of attack does it defend against?
105. What technologies and approaches are used to secure information and services deployed on cloud computing infrastructure?
106. What information security challenges are faced in a cloud computing environment?
107. Can you give me an overview of IP multicast?
108. How many bits do you need for a subnet size?
109. What is packet filtering?
110. Can you explain the difference between a packet filtering firewall and an application layer firewall?
111. What are the layers of the OSI model?
112. How would you login to Active Directory from a Linux or Mac box?
113. What is an easy way to configure a network to allow only a single computer to login on a particular jack?
114. What are the three ways to authenticate a person?

115. 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?
116. How would you compromise an “office workstation” at a hotel?
117. What is worse in firewall detection, a false negative or a false positive? And why?
118. How would you judge if a remote server is running IIS or Apache?
119. What is the difference between an HIDS and a NIDS?
120. Why is it so hard to monitor cloud traffic from the network?
121. What is SD-WAN?

Application security

122. What is CI/CD pipeline?
123. Vulnerabilities represent 50% of Application Security pen test findings, what’s the other half?
124. Can you explain what is business logic error and what does that have to do with application security?
125. Describe the last program or script that you wrote. What problem did it solve?
126. Can you briefly discuss the role of information security in each phase of the software development lifecycle?
127. How would you implement a secure login field on a high traffic website where performance is a consideration?
128. What are the various ways to handle account brute forcing?
129. What is cross-site request forgery?
130. Can you explain the hardest application security challenge you have worked with and how did you overcome that?
131. How does one defend against CSRF?
132. If you were a site administrator looking for incoming CSRF attacks, what would you look for?
133. What’s the difference between HTTP and HTML?
134. How does HTTP handle state?
135. What exactly is cross-site scripting?
136. What’s the difference between stored and reflected XSS?
137. What are the common defences against XSS?
138. You are remoted into 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?
139. On a Windows network, why is it easier to break into a local account than an AD account?
140. What does user enumeration mean?
141. Can you explain OWASP top 10?
142. How would you secure a database?
143. What are the common defences against SQL injection?
144. How do see the obfuscated SQL injection in clear text?
145. How would you secure the local access to database?

Security architect

146. Explain data leakage and give examples of some of the root causes.
147. What are some effective ways to control data leakage?
148. Describe the 80/20 rules of networking.
149. What are web server vulnerabilities and name a few methods to prevent web server attacks?
150. What are the most damaging types of malwares?
151. What's your preferred method of giving remote employees access to the company network and are there any weaknesses associated to it?
152. List a couple of tests that you would do to a network to identify security flaws.
153. What kind of websites and cloud services would you block?
154. What type of security flaw is there in VPN?
155. What is a DDoS attack?
156. Can you describe the role of security operations in the enterprise?
157. What is layered security architecture? Is it a good approach? Why?
158. Have you designed security measures that span overlapping information domains? Can you give me a brief overview of the solution?
159. How do you ensure that a design anticipates human error?
160. How do you ensure that a design achieves regulatory compliance?
161. What is capability-based security? Have you incorporated this pattern into your designs? How?
162. Can you give me a few examples of security architecture requirements?
163. Who typically owns security architecture requirements and what stakeholders contribute?
164. What special security challenges does SOA present?
165. What security challenges do unified communications present?
166. Do you take a different approach to security architecture for a COTS vs a custom solution?
167. Have you architected a security solution that involved SaaS components? What challenges did you face?
168. Have you worked on a project in which stakeholders choose to accept identified security risks that worried you? How did you handle the situation?
169. You see a user logging in as root to perform basic functions. Is this a problem?
170. What is data protection in transit vs data protection at rest?
171. You need to reset a password-protected BIOS configuration. What do you do?

Risk management

172. Is there an acceptable level of risk?
173. Is it a good idea to pay the ransom in when your data has been encrypted by a ransomware?
174. What's the most comprehensive security standard to manage risk?

175. How do you measure risk? Can you give an example of a specific metric that measures information security risk?
176. Can you give me an example of risk trade-offs (e.g. risk vs cost)?
177. What is incident management?
178. What is business continuity management? How does it relate to security?
179. What is the primary reason most companies haven't fixed their vulnerabilities?
180. What's the goal of information security within an organization?
181. What's the difference between a threat, vulnerability, and a risk?
182. 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]
183. As a corporate information security professional, what's more important to focus on: threats or vulnerabilities?
184. 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?
185. How would you build the ultimate botnet?
186. What are the primary design flaws in HTTP, and how would you improve it?
187. If you could re-design TCP, what would you fix?
188. What is the one feature you would add to DNS to improve it the most?
189. What is likely to be the primary protocol used for the Internet of Things in 10 years?
190. If you had to get rid of a layer of the OSI model, which would it be?
191. What is residual risk?
192. What is the difference between a vulnerability and an exploit?
193. What role does cyber awareness have in information security?
194. What is a tabletop exercise?
195. Can you explain threat modelling?
196. Why are the incidents relating to insiders more expensive?

Security audits, testing & incident response

197. What is the main driver for security audits and pen tests?
198. Can you explain what a great scoping process look like?
199. What is an IT security audit?
200. What is the main reason why organisations don't fix the penetration test findings?
201. What's the difference between high and critical vulnerability finding?
202. What is an RFC?
203. What is your favourite exploit?
204. What type of systems should be audited?
205. How would you bypass AV?
206. Why are the roles important when testing API's?
207. What's the difference in testing mobile and web application?
208. What's the difference in testing web application and API?
209. Have you worked in a virtualized environment?

210. What is the most difficult part of auditing for you?
211. Describe the most difficult auditing procedure you've implemented.
212. What is change management?
213. What were some of the findings in one of your last times you tested an incident response plan?
214. What types of RFC or change management software have you used?
215. What do you do if a rollout goes wrong?
216. How do you manage system major incidents?
217. How do you ask developers to document changes?
218. How do you compare files that might have changed since the last time you looked at them?
219. Can you explain the three types of network review?
220. How would you conduct a password audit?
221. Name a few types of security breaches.
222. What is a common method of disrupting enterprise systems?
223. What are some security software tools you can use to monitor the network?
224. What should you do after you suspect a network has been hacked?
225. How can you encrypt email to secure transmissions about the company?
226. What document describes steps to bring up a network that's had a major outage?
227. How can you ensure backups are secure?
228. What are your thoughts on automated penetration testing?
229. What is one way to do a cross-script hack?
230. How can you avoid cross script hacks?
231. How do you test information security?
232. What is the difference between black box and white box penetration testing?
233. What is a vulnerability scan?
234. In pen testing what's better, a red team or a blue team?
235. Why would you bring in an outside contractor to perform a penetration test?
236. What does PCI-DSS say about pen testing?
237. How would you deliver a social engineering security test?
238. Why is incident response plan important?
239. How do you test the security of cloud services like Salesforce or Amazon AWS?
240. What are the three first steps when responding to a ransomware attack?
241. What does lockpicking have to do with security testing?
242. How would you test a ATM or smart parking meter?
243. What are the you biggest bounties you have earned?
244. Can you name a few EDR tools?
245. What is your favourite physical security testing tool or device?
246. What would be the topic of phishing email if you would send it today?
247. At what stage you usually engage with the developers?
248. At what stage of development lifecycle, you should do the security testing?
249. What is the difference between security audit and penetration test?
250. Can you explain the biggest challenge while doing a security test and how did you overcome that?

251. You managed to hack the smart thermometer in casino, how would you make your way to the high-roller database and back?
252. Why is Tesla paying million dollars for bugs/vulnerabilities?

Cryptography

253. What is secret-key cryptography?
254. What is public-key cryptography?
255. What is a session key?
256. What is RSA?
257. How fast is RSA?
258. What would it take to break RSA?
259. Are strong primes necessary for RSA?
260. How large a module (key) should be used in RSA?
261. How large should the primes be?
262. How is RSA used for authentication in practice? What are RSA digital signatures?
263. What are the alternatives to RSA?
264. Is RSA currently in use today?
265. What are DSS and DSA?
266. What is difference between DSA and RSA?
267. Is DSA secure?
268. What are special signature schemes?
269. What is a blind signature scheme?
270. What is a designated confirmer signatures?
271. What is a fail-stop signature scheme?
272. What is a group signature?
273. What is blowfish?
274. What is SAFER?
275. What is FEAL?
276. What is Shipjack?
277. What is stream cipher?
278. What is the advantage of public-key cryptography over secret-key cryptography?
279. What is the advantage of secret-key cryptography over public-key cryptography?
280. What is Message Authentication Code (MAC)?
281. What is a block cipher?
282. What are different block cipher modes of operation?
283. What is a stream cipher? Name a most widely used stream cipher.
284. What is one-way hash function?
285. What is collision when we talk about hash functions?
286. What are the applications of a hash function?
287. What is trapdoor function?
288. Cryptographically speaking, what is the main method of building a shared secret over a public medium?
289. What's the difference between Diffie-Hellman and RSA?

290. What kind of attack is a standard Diffie-Hellman exchange vulnerable to?
291. What's the difference between encoding, encryption, and hashing?
292. 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?
293. What's the difference between Symmetric and Asymmetric encryption?
294. If you had to both encrypt and compress data during transmission, which would you do first, and why?
295. What is SSL and why is it not enough when it comes to encryption?
296. What is salting, and why is it used?
297. What are salted hashes?
298. What is the Three-way handshake? How can it be used to create a DOS attack?
299. What's more secure, SSL or HTTPS?
300. Can you describe rainbow tables?