SECURITY ANALYST INTERVIEW QUESTIONS

By URDU IT Academy and its Students

URDU IT ACADEMY
EDUCATION FOR ALL

website: www.urduitacademy.com

VERSION	2.0
DATE	MARCH 28, 2019
PREPARED BY	MR. KASHIF IQBAL
REVIEWED BY	MR. SOHAIB ALAM MR. ASIF SAEED

1. What type of Security you use in your Home Network?

2. What you know about global information Security policy or Information Security policy in the organisation / Does your organisation have a security policy ? If you say yes – then make sure you have read it because they might ask you leading question from there.

3. Differentiate between Vulnerability, Threat and Risk and give any real life analogy?

4. How you Secure you Windows and Linux Server ? There could be many right Answers to this question.

5. You are publishing or making one server live on web that will host your corporate Website how will you secure it? you should know how to secure the server when it is connected to DMZ and how to secure if it is hosted on Cloud Like AWS / Azure

6. What is the difference between filter and blocked ports ?

7. What ports does Ping uses ?

8. Why it is important to monitor DNS ?

9. What is the difference between MD5 , SHA1 and AES ?

10. How do you secure any services in the cloud? This is very open question and there are a lot of security feature sets in every cloud platform for Example AWS have some built in security tools like Guard duty / Trusted advisor etc.. Azure have threat monitoring on SQL Servers a part from this you can explain about the security architecture recommended by the cloud providers .

11. If you have to store a password in the database how will you store it ?

12. What is a salt in Security?

13. What is rainbow table attack and how you protect your system against it ?

14. Do you know what is OWASP can you tell me top 5 vulnerabilities published by OWASP this year ?

15. Tell me about any recent 5 vulnerabilities that are announced in the industry? If you can't answer this you are not a Security guy

16. What is SQL injection / CSRF / Cross site scripting ?

17. What is the difference between SSL and HTTPS?

18. Where do you get your cybersecurity news/ updates ?

19. Difference between IPS / IDS ?

20. Difference between Symmetric and Asymmetric Encryption?

21. Do you know about CIS benchmarking ?

22. What Vulnerability assessment tool you have worked on ?

23. What Antivirus you would prefer to use and why? Be careful on this you should back your question with good points AV-test is good place to start?

24. What is incident response?

25. You have been urgently called on the site for incident response, when you reach there as a first responder you can see Ransomware screen what would be your first steps ?

26. What is the difference between ASA And Checkpoint / Paloalto / Juniper and any other firewall ?

27. What you know about SIEM and what SIEM you have worked on ?

28. What type of security tools you have worked on?

29. What you know about threat hunting?

30. How would you respond to the system that has a malware infection?

31. Learn how Wireshark works and make sure you know how to use wireshark? sometimes the interviewer show you a wireshark output and ask you to identify any problem

32. Know the port numbers DHCP, DNS, HTTP/S and others?

33. What is the difference between FTPS and SFTP?

34. What is white-box and black-box pentesting ?

35. What is PII (Personal Identifiable Information)?

36. What you know about GDPR ?

37. You should know response codes from page like 1xx - Informational responses 2xx – Success 3xx – Redirection 4xx - Client side error 5xx - Server side error

38. What you know about Tracert / Traceroute?

39. What is DOS / DDOS and how you mitigate against it ? what is layer 7 DOS ?

40. What is WAF and what you know about it ? (Web application Firewall)

41. What is Patch Tuesday ? (If anyone don't know the answer of this I will not hire him as security analyst)

42. What is False positive / False negative / True positive and True Negative ?

43. What is the difference between Policy, Procedure and Guideline ?

44. What is the difference between Security testing and bug bounty and which one you prefer ?

45. What is the port used by ISAKMP ?

46. Explain me all the steps of Establishing IPSEC VPN ?

47. Explain me all the steps of how HTTPs communication happens between Client and Server ?

48. What does this command do "**chmod 777 ***"? Is there any security concern?

49. What does this command do in linux "**kill -9 2173**"?

50. What are iptables in Linux?

51. Familiarise yourself with Kali Linux some security analysts are expected to know this . Nmap / Wireless cracking (Aircrack) / Metasploit etc..

52. Explain OSI Layer model in as much detail you can ?

53. Name some InfoSec conferences you attend ?

54. Learn to Read and write script codes this is vital for any future cyber security analysts ?

55. What you know NIST , USCert , ISO27001 , PCI DSS ?

56. What is virtustotal ?

57. What is ARP spoofing and how you protect your network from it ?

58. What is the difference between TCP / UDP and what you prefer ?

59. One of our Staff have to visit outside the country and he want to take his company laptop with him where Cyber crime is high , what precautions you would take ?

60. How does a key logger works ?

61. What is Difference between Risk, threat ,vulnerability& exploit?

62. How to make Co-Relation for DOS, DDOS, SQL INJECTION, CROSS SITE SCRIPTING, VA.

63. How to make co-relation for a user which is not logged in from last 30 days?

64. What is a Malware ?

65. What is a TCP Flag ?

66. What is SIEM architecture ?

67. What port should be open at the time of implementing SIEM ?

68. How to check if an event is false positive or its threat ?

69. What is syslog and its 7 level ?

70. What alerts do you usually monitor and types of alerts ?

71. What is difference between SIEM and Network Forensic ?

72. What is the biggest challenge you have faced in network security so far ?

73. How would you decide which license to buy for SIEM ?

74. What troubleshooting steps you would take if a device is showing as unknown in RSA ?

75. If a cisco ASA is discovered as a Linux , what will you do ?

76. What will you check if a device is not sending logs ?

77. What are two main differences between IPS and IDS ?

78. What is TCP transport layer protocol ?
79. Video communication uses TCP od UDP ?
80. What is SYSLOG default port ?
81. What does CIA stand for ?
82. What will you do if collectors stop functioning ?
83. You don't have much experience regarding the technology we use, how will you manage it?
84. What are the reports you send on daily basis ?
85. How do you stay updated with changing technology ?
86. What are latest vulnerabilities found ?
87. Which version is vulnerable for heartbleed vulnerability ?
88. What is the difference between Local Collector and Remote Collector ?
89. The place you install a remote collector, can we call it a site ?
90. What is difference between L3 switch and a router ?
91. What is ARP poisoning ?
92. What is Smurf Attack ?
93. What is MITM, Man-in-the-Middle Attack ?
94. What is covert channel ?
95. What is a BOTNET ?
96. What is an incident ?
97. What are 7 Layers of OSI Model ?
98. What is VLAN and VTP ?
99. What are some types of routing ?
100. What is Google Hacking ?

101. What is False Positive and False negative ?
102. What is True Positive and True Negative ?
103. What is Encoding, Encryption and Hashing ?
104. What is an incident, event and problem ?
105. What is DLP ?
106. What is difference between IT Security and Information Technology?
107. What is difference between Cyber Security and Information Security?
108. What is difference between SIEM and LMI ?
109. What will you do if you saw a Zero day Attack ?
110. What is Logger and its use in arcsight ?
111. What is difference between Simple and join co-relation ?
112. What is Trend and Active list in arcsight ?
113. What is the incident handling standard process ?
114. What is routing and routed protocol ?
115. What is STP in Cisco Switch ?
116. What is broadcast and collision Domain ?
117. What is VTP in switch ?
118. What is Defence in Depth ?
119. What is Source Routing and why don't we use it ?
120. What is ping and traceroute and how does it work ?
121. What is the difference between tracert command used in windows and linux ?
122. What is the difference between port scan and vulnerability scan ?
123. How do you prevent DDOS attack ?

124. What is the difference between CORR and Database ?

125. How would you bypass ASLR ?

126. How would you bypass SafeSEH ?

127. Explain the behaviour and your analysis methodology of any new APT.

128. What is DEP ? How can it be bypassed ?

129. Explain a PE file ?

130. What is code injection ?

131. What APIs are used by Malware to connect to the server ?

132. How can you unpack a malware and in how many ways?

133. In what way malware try to evade analysis?

134. Explain the anti-debugging techniques employed by a macro malware.

135. What are different types of breakpoints , what is their use and when to use those breakpoints ?

136. Describe what buffer overflow is and how you would test for it ?

137. What is SMB and how to exploit it ?

138. How do UAF Exploits work ?

139. What is difference between Symmetric and Asymmetric encryption ?

140. In public-Key Cryptography which key is sued for what function ?

141. Which algorithm is better than other? AES-128, AES-256, AES 196.

142. What is difference between CBC mode and EBC mode of encryption ?

143. What is a Windows Portable Executable ?

144. What is ESP register used for in the Intel x86-32 architecture ?

145. What is primary reason to not upload targeted malware to VT ?

146. What DFIR evidence do you gather first and why ?

147. Assume a user forwards you a suspected phishing email, how do you respond and handle it ?

148. What percentage of malware in the wild do you think AV can detect ?

149. Explain to me why you need to consider scope in the identification stage of IR?

150. What is the primary problem with bash history as a forensic artefact and name one way to partially recreate this data during investigation.

151. How will you determine a malicious file without executing it ?

152. How will malware try to evade analysis and in how many ways ?

153. Name at least 3 different vulnerability scanners.

154. How would you validate a false positive and negative ?

155. How would you design and execute an incident response plan ?

156. What information would you include in a SOC report ?

157. Describe how TCP handshake works .

158. Name four types of DNS records and what they signify.

159. You got a report that your company LAMP website maybe being DDOOSED. How do you investigate ?

160. What will be your approach to implement a new SIEM?

161. Explain difference between Local and Network authentication and walk me through authentication process.

162. What will be your primary data sources in detecting botnet activity ?

163. What is a dis-advantage of signature based malware detection ?

164. What is Cross-Site Request Forgery ?

165. In what category XXE falls ?

166. How can SQL injection lead to remote code execution ?

167. I have a /24 subnet of hosts on the internet that I would like to pen-test. Take me through all the assessment detail steps.

168. On assessment you have just compromised a Mac OS X laptop inside a corporate user subnet. Your goal is to infiltrate Active Directory hashes from the AD server. How do you accomplish this ?

169. During the penetration test, you find an instance of Outlook Web Access belonging to the client. Describe how you would attack this .

170. You are performing an onsite penetration test. You don't want to perform an active scanning. How would you gather credentials ?

171. How would you target a database that you know lie behind a jump server with unknown IP address?

172. Describe last programme/script you wrote . what problems did it solve ?

173. What kind of attacks are you vulnerable to when you use weak ciphers.

174. What is pivoting? Why an attacker uses this technique?

175. Which department in a company is most likely to be attacked?

176. What are some of the low-hanging fruits you go after as a pen tester?

177. Describe three of most common ways an external attacker might try to gain access to network .

178. How would bypass a network IDS ?

179. What leg of CIA tirade is the most important ?

180. Two factor authentication protects against session hijacking . True or False? Explain.

181. How would you explain a business user why we are not giving them Local Admin to their machine ?

182. Walk me through if you are a threat actor, how would you compromise an organisation in all three domains?(Physical, Digital and Human).

183. Name three internet protocol which uses TCP, three with UDP and name two which use neither and what port they run.

184. If you had to encrypt and compress data during communication, which would you do first and why ?

185. In public-key cryptography, you have a public and private key, and you often perform encryption and signing functions. Which key is used for which function ?

186. What are the advantages offered by Bug Bounty ?

187. Who do you look upto in the field of information security and why ?

188. Who is more dangerous to an organisation , insiders or outsiders?

189. You just stepped on the elevator with your CEO. They ask you how secure are we? What would you say ?

190. You have an unlimited budget and resources. Please draw the most secure corporate network for my organisation. It must have specific components including but not limited to : The Internet, one user subnet, at least one Active Directory server, one web server(with backend database) on the Internet, one HR Server , WIFI for users and a VPN.

191. Design a infrastructure to run a web application and database and the components you choose should have following characteristics:
    a. Open Source (Free)
    b. Secure
    c. Scalable

Best of Luck