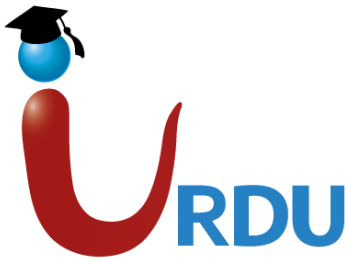
Security Analyst Interview Questions

By URDU IT Academy and its Students



Prepared by: - Kashif Iqbal

01/06/2018

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 me 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. What 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 e.t.c 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? 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 profer to use and why? Becareful 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 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 you respond to the system that has a malware infection?

31. Understand how Wireshark works and make sure you know how to use wireshark ? sometimes the interviewer show you 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 whitebox 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 ip tables in Linux

51. Familiarise yourself with Kali Linux some security analysts are expected to know this . Nmpa / Wireless cracking / metaexploit e.t.c

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

53. Name some InfoSec conference 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 visist 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 ?