TOP INTERVIEW QUESTIONS FOR APPLICATION SECURITY

LinkedIn
@sahilgupta3112

Save it For Later

Encryption and Authentication

1. What is a three-way handshake?
2. How do cookies work?
3. How do sessions work?
4. Explain how OAuth works.
5. What is a public key infrastructure flow and how would I diagram it?
6. Describe the difference between synchronous and asynchronous encryption.
7. Describe SSL handshake.
8. How does HMAC work?
9. Why HMAC is designed in that way?
10. What is the difference between authentication vs authorization name spaces?
11. What’s the difference between Diffie-Hellman and RSA?
12. How does Kerberos work?
13. If you're going to compress and encrypt a file, which do you do first and why?
14. How do I authenticate you and know you sent the message?
15. Should you encrypt all data at rest?
16. What is Perfect Forward Secrecy?

Network Level and Logging - 1

1. What are common ports involving security, what are the risks and mitigations?
2. Which one for DNS?
3. Describe HTTPs and how it is used.
4. What is the difference between HTTPS and SSL?
5. How does threat modeling work?
6. What is a subnet and how is it useful in security?
7. What is subnet mask?
8. Explain what traceroute is.
9. Draw a network, then expect them to raise an issue and have to figure out where it happened.
10. Write out a Cisco ASA firewall configuration on the white board to allow three networks unfiltered access, 12 networks limited access to different resources on different networks, and 8 networks to be blocked altogether.
11. Explain TCP/IP concepts.
12. What is OSI model?
13. How does a router differ from a switch?

Network Level and Logging - 2

14. Describe the Risk Management Framework process and a project where you successfully implemented compliance with RMF.
15. How does a packet travel between two hosts connected in same network?
16. Explain the difference between TCP and UDP.
17. Which is more secure and why?
18. What is the TCP three way handshake?
19. What is the difference between IPSEC Phase 1 and Phase 2?
20. What are biggest AWS security vulnerabilities?
21. How do web certificates for HTTPS work?
22. What is the purpose of TLS?
23. Is ARP UDP or TCP?
24. Explain what information is added to a packet at each stop of the 7 layer OSI model.
25. Walk through a whiteboard scenario for your environment of choice (Win/Linux) in which compromising the network is the goal without use of social engineering techniques (phishing for credential harvesting, etc).

Network Level and Logging - 3

26. Explain how you would build a web site that could secure communications between a client and a server and allow an authorized user to read the communications securely.
27. How does an active directory work?
28. Do you know how Single Sign-On works?
29. What is a firewall?
30. How does it work?
31. How does it work in cloud computing?
32. Difference between IPS and IDS?
33. How do you build a tool to protect the entire Apple infra?
34. How do you harden a system?
35. How to you elevate permissions?
36. Describe the hardening measures you've put on your home network.
37. What is traceroute? Explain it in details.
38. How does HTTPS work?
39. What would do if you discovered an infected host?
40. What is SYN/ACK and how does it work?

OWASP Top 10, Pentesting and/or Web Applications

1. Differentiate XSS from CSRF.
2. What do you do if a user brings you a pc that is acting 'weird'? You suspect malware.
3. What is the difference between tcp dump and FWmonitor?
4. Do you know what XXE is?
5. Explain man-in-the-middle attacks.
6. What is a Server Side Request Forgery attack?
7. Describe what are egghunters and their use in exploit development.
8. How is pad lock icon in browser generated?
9. What is Same Origin Policy and CORS?

Databases

1. How would you secure a Mongo database?
2. Postgres?
3. Our DB was stolen/exfiltrated. It was secured with one round of sha256 with a static salt.
   I. What do we do now?
   II. Are we at risk?
   III. What do we change?
4. What are the 6 aggregate functions of SQL?

Tools and Games

1. Have I played CTF?
2. Would you decrypt a steganography image?
3. You're given an ip-based phone and asked me to decrypt the message in the phone.
4. What CND tools do you knowledge or experience with?
5. What is the difference between nmap -ss and nmap -st?
6. How would you filter xyz in Wireshark?
7. Given a sample packet capture - Identify the protocol, the traffic, and the likelihood of malicious intent.
8. If left alone in office with access to a computer, how would you exploit it?
9. How do you fingerprint an iPhone so you can monitor it even after wiping it?
10. How would you use CI/CD to improve security?
11. You have a pipeline for Docker images. How would you design everything to ensure the proper security checks?
12. What technical skill or project are you working on for fun in your free time?
13. If you had to set up supply chain attack prevention, how would you do that?

Programming and Code

1. Code review a project and look for the vulnerability.
2. How would you conduct a security code review?
3. How can Github webhooks be used in a malicious way?
    - If I hand you a repo of source code to security audit what's the first few things you would do?
        - Can I write a tool that would search our Github repos for secrets, keys, etc.?
    - Slack?
        - https://arstechnica.com/security/2016/04/hacking-slack-accounts-as-easy-as-searching-github/
    - AWS?
    - Etc.
4. Given a CVE, walk us through it and how the solution works.
5. Tell me about a repetitive task at work that you automated away.
6. How would you analyze a suspicious email link?

Compliance

1. Can you explain SOC 2?
   - What are the five trust criteria?
2. How is ISO27001 different?
3. Can you list examples of controls these frameworks require?
4. What is the difference between Governance, Risk and Compliance?
5. What does Zero Trust mean?
6. What is role-based access control (RBAC) and why is it covered by compliance frameworks?
7. What is the NIST framework and why is it influential?
8. What is the OSI model?