Interview Prep

How to trick tech corps into paying you a salary

Andrew Lebedinsky

outline

1. General tips
2. Live interviews
3. Good answers to common questions

Part 1: General Tips

what kind of interview will we prep for?

- Technical interview
- For an internship position
- Specifically a security role
    - We will mostly focus on red team

what do interviewers want?

- "Does this person know shit"
  - If you're in BK, you do
- "Does this person care about security"
- "Is this person cool"

"does this person know shit"

- Generally evaluated in two ways:
  - The good way
  - The bad way
- The good way is to ask open-ended theoretical questions
- The bad way is to ask trivia questions ("what is Port 22?")

trivia you need to know

- OWASP Top 10 - https://owasp.org/www-project-top-ten/
- CVE database (may it rest in peace)
- MITRE ATT&CK
- Specific common web vulns + their **impacts and mitigations**
    - XSS (reflected vs. stored vs. DOM)
    - SQL injection
    - Path traversal
    - SSRF
    - CSRF
    - Local File Inclusion
    - IDOR
    - Useful bonuses: Deserialization, JWTs, XXE

more trivia

- Binary exploitation:
  - Buffer overflows
  - Heap vulns
  - ASLR, stack canaries
- Cryptography
  - Symmetric vs. asymmetric
  - General idea behind RSA, AES, Diffie-Hellman
  - (bonus) a couple of specific attacks (CBC bit-flipping, padding oracles, etc.)

networking trivia

- Common port numbers - 22, 53, 80, 443
- Protocols
  - HTTP vs. HTTPS
  - TLS vs. SSL
  - UDP vs. TCP
  - SSH
  - FTP
  - IPv4 vs. IPv6
  - Unironically, just go through every protocol in the panel on the side of https://en.wikipedia.org/wiki/OSI_model

general resources

- Portswigger Web Security Academy: https://portswigger.net/web-security/all-materials
- Hacktricks: https://book.hacktricks.wiki/en/pentesting-web/web-vulnerabilities-methodology.html
- BK Discord + pinned messages
- This trivia stuff does unironically just require grinding it out and cramming like for an exam

soft skills for trivia questions

- If you don't know the answer, **don't try to bullshit**
    - "I'm not sure but do you want me to take a guess?"
    - Nothing is more of a red flag than someone who is confidently wrong
    - If the interviewer tells you the right answer, demonstrate interest

theoretical questions

- Generally have two types of structure:
  - "Suppose you're doing X, how would you go about it?"
  - "Describe how Y works."
- The more detail you can give, the better!
- If you're unsure if they wanna hear about some part, **just ask**
- **Ask clarifying questions before you start answering**
  - Useful for you, and also shows you understand important nuances

preparing for theoretical questions

- **Hands-on experience is everything**
- HackTheBox, bug bounties, CTFs, CCDC, personal projects, etc.
- There are some really common ones that you can just memorize

other tips

- Be friendly! Chat with your interviewer, make a good impression.
- Have some interesting stuff in your video background
- Ask follow-up questions at the end
  - "Do you have any security news sites you recommend?"
  - Be prepared to talk about some cool news you saw as well
  - "What does your job look like day-to-day?"
- If you have cool projects, clubs, etc. on your resume (and you should), be ready to yap about them!

██ Part 2: Interview Time

██ Part 3: Good Interview Answers

questions - red team

- Suppose you see a social media site...
  - How might you model the threats to it?
  - How might you hack it?
  - How might you mitigate these potential problems?
- What happens when you type google.com and press "enter"?
- How would you perform recon on an organization?
- You're given an unknown file. What do you do to figure out what it does?

questions - blue team

- Here's a social media site with feature set XYZ, what controls should be put in place as it's being designed?
- The site is built and you're going to get pentested for the first time. What do you do?
- AAAAAAAA!! The site went live and someone got RCE on the API server? How do you fix this?
- Okay we kicked the hacker out, how should we follow up on this incident?