面经题库十三香

1、自我介绍

1. 自我介绍
2. 谈谈你的职业发展规划
3. 擅长哪块技能，未来想往哪方向去深入？
4. 最近有在研究什么新的漏洞吗？
5. 你自己最大的优点和缺点是什么？
6. 前段实习做了些什么？
7. 你愿意加班吗？
8. 为什么投我们公司？
9. 你觉得有哪些是你会别人不会的？
10. 为什么想要应聘这个岗位？
11. 进入部门后，你需要多长时间进入项目？
12. 对上司有什么要求？喜欢和什么样的领导合作？

2、设备

13. 了解的厂商设备有哪些？
14. IDS 和 IPS 的区别是什么？
15. 设备误报如何处理？
16. 对蜜罐有什么了解？
17. 安全设备、流量监控设备有了解吗？
18. 天眼常用的语法有哪些？
19. 平时天眼分析是怎么分析和处置流程的？
20. 你在天眼上发现一条告警如何尝试去溯源？

3、流量分析

21. shiro 流量分析
22. 有没有流量分析的经验？（举例说明）
23. 用 Wireshark 进行流量分析的流程

4、应急响应

24. 应急响应的基本思路是什么？
25. 你知道哪些常用的威胁情报平台？
26. 应急响应如何查找挖矿病毒，如何通过进程找到挖矿文件？

27. 有处理过勒索和挖矿的经验吗？
28. 请谈谈常见的应急排查方式。
29. 常见的应急响应时间分类。
30. Web 服务器被入侵后，怎样进行排查？

5、渗透测试

31. 描述外网打点的流程
32. 判断出靶标的 CMS，对外网打点有什么意义？
33. log4j2 的漏洞原理
34. 如何建立隐藏用户？
35. 代码执行、文件读取、命令执行的函数有哪些？
36. 正向 shell 和反向 shell 的区别是什么？
37. OWASP TOP 10 漏洞有哪些？
38. SQL 注入的种类有哪些？
39. 常见的中间件有哪些？他们有那些漏洞？
40. 渗透测试流程？
41. shiro 漏洞原理及其特征？
42. Fastjson 反序列化漏洞原理？
43. shiro721 和 550 区别和原理？
44. 请阐述 CRLF 攻击原理？
45. redis 未授权漏洞利用？
46. CDN 和 DNS 区别？CDN 绕过思路？
47. WAF 绕过的手法你知道哪些？
48. 命令无回显如何解决？

6、溯源反制

49. 溯源反制的手段有哪些？
50. 如何定位到攻击 IP？
51. 假设发现 web 应用服务器发现文件异常增多，初步怀疑被上传 webshell，描述一下流量分析溯源思路？
52. wireshark 简单的过滤规则
53. Webshell 流量交互的流量特征？

7、工具

54. 常见的 webshell 检测工具有哪些？
55. 常见的目录扫描工具有哪些？
56. 蚁剑/菜刀、冰蝎的相同和不同之处
57. SQLMap 自带脚本你知道哪些？有编写过吗？

58. 你常用的渗透工具 or 漏扫工具有哪些？
59. SQLMap 中——os-shell 的原理及利用条件？
60. 信息收集你会使用哪些工具？具体用来干什么？
61. Nmap 常用参数，说一下？
62. 讲讲常见的代码审计工具原理
63. shiro 反序列化工具的原理
64. 不用 SQLMap 情况下 SQL 注入点如何找？

8、内网

65. 内网不出网如何判断？
66. 内网渗透流程？
67. 域信息收集思路有哪些？
68. 代理转发常用的工具有哪些？
69. 正向代理和反向代理的区别是什么？
70. 有做过免杀吗？
71. 知道免杀的思路吗？
72. MSF 了解过吗？
73. 什么是内网穿透？

9、系统方面

74. 如何判断靶标站点时 windows/Linux？
75. windows 常见的提权方法有哪些？
76. linux 常见的提权方法有哪些？
77. windows 加固方法有哪些？
78. linux 加固方法有哪些？
79. linux 如何发现网络连接
80. linux 如何查看进程？
81. 常见日志 看日志看哪几个文件 文件目录？

10、SRC

82. 有没有挖过 SRC？
83. 在哪些 SRC 平台上提交过漏洞？
84. 能说一下常见的逻辑漏洞有哪些吗？
85. 看你有些 cnvd 和 cve，讲讲挖洞的过程
86. 讲几个印象深刻的挖洞经历
87. 平时在哪里挖漏洞？挖了多久？
88. 主要挖哪些类型的漏洞？有排名吗？

11、比赛

89. 参加过哪些比赛？
90. 你在（比赛中）担任什么？
91. 说说 CTF 你都做哪些题型？
92. 有打过知名的 CTF 吗？讲讲经历
93. 说一个印象深刻的 CTF 题目

12、在校经历

94. 你是怎么接触安全的？
95. 你才大二或大三，你在学校是怎么自学安全的？
96. 近期的学习规划是什么？
97. 你现在的学习内容（方向）是什么？
98. 你学校成绩如何，有挂科的吗？
99. 你获取网络安全知识途径有哪些？

13、证书

100. 讲一讲你考过的证书都学到了些什么？