0x00 前言

随着科学技术的发展，网络安全已经提升到了国家层面。习大大说：“没有网络安全就没有国家安全。”那么在网络安全大热的今天，如何才能历经重重磨难才能达到公司需要的高度，才能符合面试官的口味,才能在众多才子中脱颖而出尼？那就好好看看博主这篇面试宝典吧，内容均是从网络上采集或者自己总结，有问题希望大家可以指出，一起进步！nice~

0x01 简述漏洞挖掘的思路

1. 1 信息收集

服务器的相关信息（真实ip，系统类型，版本，开放端口，WAF等）

网站指纹识别（包括，cms，cdn，证书等），dns记录

whois信息，姓名，备案，邮箱，电话反查（邮箱丢社工库，社工准备等）

子域名收集，旁站，C段等

google hacking针对化搜索，pdf文件，中间件版本，弱口令扫描等

扫描网站目录结构，爆后台，网站banner，测试文件，备份等敏感文件泄漏等

传输协议，通用漏洞，exp，github源码等

1.2 漏洞挖掘

浏览网站，看看网站规模，功能，特点等

端口，弱口令，目录等扫描,对响应的端口进行漏洞探测，比如 rsync,心脏出血，mysql,ftp,ssh弱口令等。

XSS，SQL注入，上传，命令注入，CSRF，cookie安全检测，敏感信息，通信数据传输，暴力破解，任意文件上传，越权访问，未授权访问，目录遍历，文件 包含，重放攻击（短信轰炸），服务器漏洞检测，最后使用漏扫工具等

1.3 漏洞利用&权限提升

mysql提权，serv-u提权，oracle提权

windows 溢出提权

linux脏牛,内核漏洞提权

1.4 清除测试数据&输出报告

日志、测试数据的清理

总结，输出渗透测试报告，附修复方案

1.5 复测

验证并发现是否有新漏洞，输出报告，归档

0x02 面试题（一）

2.1 拿到一个待检测的站，你觉得应该先做什么？

2.1.1 信息收集

1、获取域名的whois信息,获取注册者邮箱姓名电话等，丢社工库里看看有没有泄露密码，然后尝试用泄露的密码进行登录后台。用邮箱做关键词进行丢进搜索引擎。利用搜索到的关联信息找出其他邮箱进而得到常用社交账号。社工找出社交账号，里面或许会找出管理员设置密码的习惯 。利用已有信息生成专用字典。

2、查询服务器旁站以及子域名站点，因为主站一般比较难，所以先看看旁站有没有通用性的cms或者其他漏洞。

3、查看服务器操作系统版本，web中间件，看看是否存在已知的漏洞，比如IIS，APACHE,NGINX的解析漏洞

4、查看IP，进行IP地址端口扫描，对响应的端口进行漏洞探测，比如 rsync,心脏出血，mysql,ftp,ssh弱口令等。

5、扫描网站目录结构，看看是否可以遍历目录，或者敏感文件泄漏，比如php探针

6、google hack 进一步探测网站的信息，后台，敏感文件

如何扩大攻击面呢？

1.收集尽量全的企业域名（包括各种子域名以及子公司的域名，越全越好）

2.收集尽量全的企业申请的公网 IP

3.对所有收集到的域名以及 IP 地址进行端口扫描（由于时间可能比较久，所以可以

选择利用 zoomeye、shodan、censys 等平台）

4.针对不同的服务进行对应的渗透测试（尤其是可能存在漏洞的中间件）

0x03 大佬面试经历

3.1 360奇安信绿盟深信服等公司秋招面试题总结与分享

3.3.1 360

讲讲渗透经验与成果

给你一个站怎么验（讲到sql注入被打断）

mysql和mssql是否了解（选了mysql）

sql注入某参数（忘了）过滤应如何绕过

sqlmap的tamper有没有自己写过

sql注入写shell的前提、方法、指令

过WAF的方法（要求详细说，用什么符号，怎么用）

phpmyadmin提权思路

挖过哪些逻辑漏洞

给一个登录框，问验证漏洞的思路

常用的信息收集方法

怎么验证是否有CDN

如何绕过CDN查真实IP

同源策略原理是什么，如何绕过同源策略

为什么同源策略无法防御csrf？

B站与A站不同源的情况下如何从B站获取到A站用户信息

ARP攻击原理，防御方法

java与php的反序列原理，如何实现

sqImap osshell原理?

sqlmap udf原理?

如何只用mysq|执行系统命令?

黄金票据有了解吗?

目标主机只开了139能否利用永恒之蓝?

你入侵了一台非域成员主机，如何快速定位

其他是域成员的主机?

PHP的站限制了任何php文件上传，如何上个

php文件? (排除截断 复写数字大小写)

waf怎么绕?

你拿到了server03的hash怎么利用?

mimikatz抓密码的原理?

不用mimikatz怎么抓明文密码?

server12限制了抓取明文密码，怎么绕过?

你有一-个webshell但无法执行系统命令，无上传，怎么进行内网渗透?

你是域成员，如何拿到域控制器?

你横向渗透常用手法有哪些?

regorge有了解过吗、它的工作原理是什么?

你发现了一个mysql的延时注入如何提高速

xxe的原理是什么?背一下xxe。

哪些会受同源策略的影响?

最近的redisRCE有了解吗?它的原理是什么

你拿到了redis未授权，你会怎么利用?

你通过java站入侵了Windows，你Windows什么权限？

你拿到了域控制器你会怎么样维持权限？

360是最早给面试机会的，当时愣头青什么也没准备就去了，一面直接凉凉，流程是一站式面试，当天给结果。另附一份哥们的社招总结，面的好像是360政企

3.3.2 奇安信

基本跟360的套路差不多，owasp top10挑一些问漏洞原理和修复方法，渗透流程，提权，内网，结合一些网络（同源策略、CDN）以及编程（漏洞扫描器的编写，爬虫去重）的问题，另外比较关注src和漏洞挖掘成果。当时前面渗透测试的部分答的都算顺利，然后问到了简历上两个写上去为了装逼的项目，因为有夸大成分所以答得不甚理想，面试官应该觉得不诚实或者太水，GG

3.3.3 绿盟

burp工具都有哪些用途，用到哪些模块

在漏洞平台上提交过哪些洞，什么原理

研究生期间的科研项目是否与安全相关，具体介绍一下

详细讲讲你简历上的渗透项目，然后根据内容问了其中一些漏洞挖掘的细节。

3.3.4 深信服

sql注入分类，宽字节注入原理。

你的渗透经验。

挖了哪些洞，怎么挖的。

ctf打过哪些比赛，讲讲web中的上传题的类型和绕过方法

如果让你用工具进行代码审计一个cms的上传功能，你会关注哪些函数

php代码审计中命令执行你会关注哪些函数，代码执行你会关注哪些函数

内网渗透怎么获取服务器账号密码

内网渗透怎么维权

python代码正则

用python实现https请求中的一些坑

**感觉深信服问的又细又广，真的是问到怀疑人生，当时答完觉得不太理想，不过后来也给了终面通知。**

3.3.5 终面

基本都是一些人事问题：

口才展示（自我介绍，项目介绍，讲讲你学生生涯最得意的两件事）

查户口（家哪的，父母干啥的，有没有女朋友\老婆，想在哪干）

性格测验（说出自己三个优点两个缺点，说出你最尊重的三个人，为什么）

压力测试（diss一下你的弱项，一个问题一直怼，考一考应变能力）

剩下的就是讨论一下薪资、进去之后的发展之类的。