护网行动 | 信息安全面试题目汇总

海绵行动

“像海绵吸水一样学习。”

前言

大家好，我们鸽了这么久的「信息安全面试题目」终于肝出来了。我们把收集的面试题目进行了二次整理，还是以红队攻击方、蓝队防守方的视角进行分类归档。如果内容当中出现错误，劳烦大家通过「海绵行动」微信公众号后台进行留言告知，我们会在后续的整理工作中进行修正。Thanks ♪(･ω･)ﾉ

海绵行动
SPONGE

“唬住就50k，唬不住就5k。”

-- 鲁 迅

描述一下外网打点的基本流程？

外网打点的基本流程主要分为：靶标确认、信息收集、漏洞探测、漏洞利用、权限获取，其最终目的是为了获取靶标的系统权限/关键数据。而在整个打点流程中，信息收集较为重要。掌握靶标情报越多，后续就能够尝试更多的攻击方式进行打点。比如：钓鱼邮件、Web漏洞、边界网络设备漏洞、弱口令等等。

在外网打点过程中，常用的信息收集工具有哪些?

名称	描述
ENScan	企业信息查询工具
Oneforall	子域名收集工具
水泽	信息收集自动化工具
FOFA、Goby	网络空间资产检索\攻击面测绘工具
Masscan	端口扫描工具
ARL 资产安全灯塔	快速侦察与目标关联的资产工具

举几个FOFA在外网打点过程中的使用小技巧?

示例	搜索语句
后台挖掘	title="后台" && body="password" && host="x.cn"
子域名	title!="404" && title!="302" && host="x.cn"
C段	ip="x.x.x.x/24" && body="password" [登录场景]
框架特征	body="icon-spring-boot-admin.svg" [Spring Boot Admin]
漏洞	body="Index of /" [列目录漏洞]

Red Team

如何识别CND?

a. 通过“ping”命令，看执行回显情况。

b. Windows系统环境下，使用“nslookup”进行查询，看返回的域名解析情况。

c. 超级PING工具，比如：all-tool.cn/Tools/ping。[看IP结果]

Red Team

邮件钓鱼的准备工作有哪些?

a. 确定邮件钓鱼的形式：链接、文件
b. 收集目标相关邮箱
c. 编写钓鱼邮件文案
d. 匿名邮箱
e. 木马免杀测试、钓鱼站点搭建
f. 反溯源

Red Team

判断出靶标的CMS，对外网打点有什么意义？

a. 判断当前使用的CMS是否存在Nday，尝试利用公开的POC、EXP进行测试。

b. 根据CMS特征关联同CMS框架站点，进行「敏感备份文件」扫描，有可能获取到站点备份文件。尝试从CMS源码进行代码审计，挖掘潜在漏洞。

Red Team

Apache Log4j2的漏洞原理是什么?

由于Log4j2组件在处理程序日志记录时存在JNDI注入缺陷，未经授权的攻击者利用该漏洞，可向目标服务器发送精心构造的恶意数据，触发Log4j2组件解析缺陷，实现目标服务器的任意代码执行，获得目标服务器权限。

Red Team

水坑攻击和鱼叉攻击的区别是什么?

水坑攻击指的是黑客通过分析被攻击者的网络活动规律，寻找被攻击者经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待被攻击者来访时实施攻击。

鱼叉攻击则是通常是指利用木马程序作为电子邮件的附件，发送到目标电脑上，诱导受害者去打开附件来感染木马。

Red Team

如何手工判断靶标站点是Windows/Linux?

a. 大小写检测：Windows大小写不敏感，而Liunx大小写敏感

b. PING指令：根据TTL值，Windows一般情况下>100、Linux则<100

Red Team

无法连接服务器3389端口的几种情况?

a. 3389端口处于关闭状态

b. 远程桌面默认端口号已被修改

c. 防火墙拦截

d. 处于内网环境

e. 超过了服务器最大连接数

f. 管理员设置了权限，指定用户才能通过3389端口进行远程桌面访问

Red Team

如何建立隐藏用户?

a. net user test$ 123456 /add [建立隐藏用户]

b. net localgroup administrators test$ /add [将隐藏用户加入管理组]

Red Team

为什么Mysql数据库的站点，无法连接?

a. 站库分离

b. 3306端口未对外开放

c. Mysql默认端口已被修改

Red Team

文件上传功能的检测点有哪些?

a. 客户端JavaScript检测（文件后缀名检测）

b. 服务端检测（MINE类型检测、文件后缀名、文件格式头）

Red Team

常见的未授权访问漏洞有哪些?

a. MongoDB 未授权访问漏洞
b. Redis 未授权访问漏洞
c. Memcached 未授权访问漏洞
d. JBOSS 未授权访问漏洞
e. VNC 未授权访问漏洞
f. Docker 未授权访问漏洞
g. ZooKeeper 未授权访问漏洞
h. Rsync 未授权访问漏洞

Red Team

代码执行、文件读取、命令执行的函数有哪些?

类型	函数
文件执行	eval、call_user_func、call_user_func_array等
文件读取	fopen()、readfile()、fread()、file()、show_source()等
命令执行	system()、exec()、shell_exec()、passthru()、pcntl_exec()等

Red Team

正向Shell和反向Shell的区别是什么?

类型	说明
正向Shell	攻击者连接被攻击者机器，可用于攻击者处于内网，被攻击者处于公网的情况。
反向Shell	被攻击者主动连接攻击者，可用于攻击者处于外网，被攻击者处于内网的情况。

Red Team

正向代理和反向代理的区别？

类型	说明
正向代理	当客户端无法访问外部资源的时候（比如Google、YouTube），可以通过一个正向代理去间接地访问。正向代理是一个位于客户端和原始服务器(origin server)之间的服务器，为了从原始服务器取得内容，客户端向代理发送一个请求并指定目标(原始服务器)，然后代理向原始服务器转交请求并将获得的内容返回给客户端。
反向代理	客户端是无感知代理的存在，以代理服务器来接受internet上的连接请求，然后将请求转发给内部网络上的服务器，并将从服务器上得到的结果返回给internet上请求连接的客户端。此时代理服务器对外就表现为一个服务器。

Red Team

Web TOP 10漏洞有哪些?

1. SQL注入
2. 失效的身份认证
3. 敏感数据泄露
4. XML外部实体（XXE）
5. 失效的访问控制
6. 安全配置错误
7. 跨站脚本（XSS）
8. 不安全的反序列化
9. 使用含有已知漏洞的组件
10. 不足的日志记录和监控

Red Team

SQL注入的种类有哪些?

a. 按照注入点类型分为：数字型、字符串、搜索型

b. 按照数据提交的方式分为：GET型、POST型、Cookie型、HTTP 头

c. 按照执行效果分为：基于报错、基于布尔的盲注、基于时间的盲注、基于数字

Red Team

常见的中间件有哪些？它们有哪些漏洞？

- IIS：PUT漏洞、短文件名猜解、远程代码执行、解析漏洞
- Apache：解析漏洞、目录遍历
- Nginx：文件解析、目录遍历、CRLF注入、目录穿越
- Tomcat：远程代码执行、war后门文件部署
- JBoss：反序列化漏洞、war后门文件部署
- WebLogic：反序列化漏洞、SSRF任意文件上传、war后门文件部署
- Apache Shiro反序列化漏洞： Shiro rememberMe（Shiro-550）、Shiro Padding Oracle Attack(Shiro-721)

Red Team

常用的目录扫描工具有哪些?

- 御剑
- Dirsearch
- dirmap
- Webdirscan

Red Team

Windows常用的提权方法有哪些?

- 系统内核溢出漏洞提权
- 数据库提权
- 错误的系统配置提权
- 组策略首选项提权
- WEB中间件漏洞提权
- DLL劫持提权
- 滥用高危权限令牌提权
- 第三方软件/服务提权等

Red Team

蚁剑/菜刀/C刀/冰蝎的相同与不相同之处

	说明
相同	都是用来连接Web Shell的工具。
不相同	相比于其他三款，冰蝎有流量动态加密。

Red Team

Windows环境下有哪些下载文件的命令?

a. certutil -urlcache -split -f [url]
b. bitsadmin /transfer myDownLoadJob /download /priority normal [url] [存放路径]
c. powershell (new-object Net.WebClient).DownloadFile([url],[存放路径])

Red Team

常见的端口有哪些？攻击点有哪些？

服务	端口号	攻击点
FTP	20、21	匿名上传下载、嗅探、爆破
Telnet	23	嗅探、爆破
SSH	22	爆破
Telnet	23	嗅探、爆破
sql server	1433	注入、弱口令、爆破
Oracle	1521	注入、弱口令、爆破
WebLogic	7001	Java反序列化、弱口令
Redis	6379	未授权访问、弱口令爆破
jboss	8080	反序列化、控制台弱口令
Zabbix	8069	远程执行、SQL注入

Blue Team

木马驻留系统的方式有哪些?

a. 注册表

b. 服务

c. 启动目录

d. 计划任务

e. 关联文件类型

Blue Team

常用的威胁情报平台有哪些?

名称	网站
Viurstotal	virustotal.com
微步威胁情报中心	x.threatbook.cn
360威胁情报中心	ti.360.cn
奇安信威胁情报中心	ti.qianxin.com
绿盟威胁情报中心	nti.nsfocus.com
安恒威胁情报中心	ti.dbappsecurity.com.cn
VenusEye威胁情报中心	venuseye.com.cn

Blue Team

常用的Webshell检测工具有哪些?

a. D盾

b. 河马WEBSHELL

c. 百度 WEBDIR+

d. Web Shell Detector

e. Sangfor WebShellKill [深信服]

f. PHP Malware Finder [支持Linux]

Blue Team

一般情况下，哪些漏洞会高频被用于打点?

a. Apache Shiro 相关漏洞

b. Fastjson 漏洞

c. Log4j

d. 上传漏洞

e. 边界网络设备资产 + 弱口令

Blue Team

Windows常用的命令有哪些?

命令	描述
type	显示文件内容
dir	显示当前目录内容
ipconfig	查看IP地址
net user	查看用户
netstat	查看端口
tasklist	查看进程列表
find	文件中搜索字符串
ping	检测网络连通情况

Blue Team

应急响应的基本思路是什么?

a. 收集信息：收集告警信息、客户反馈信息、设备主机信息等

b. 判断类型：安全事件类型判断。（钓鱼邮件、Webshll、爆破、中毒等）

c. 控制范围：隔离失陷设备

d. 分析研判：根据收集回来的信息进行分析

e. 处置：根据事件类型进行处置（进程、文件、邮件、启动项、注册表排查等）

f. 输出报告

Blue Team

Linux常用的命令有哪些?

命令	描述
cat	显示文件内容
ls	显示当前目录内容
ifconfig	查看IP地址
whoami	查看当前用户
netstat	查看端口
ps	查看进程列表
grep	文件中搜索字符串
ping	检测网络连通情况
crontal	检查定时任务

Blue Team

蓝队常用的反制手段有哪些?

a. 蜜罐

b. 对攻击目标进行反渗透（IP定位、IP端口扫描、Web站点渗透）

c. 应用漏洞挖掘&利用（菜刀、Goby、Xray、蚁剑）

d. id -> 社交特征关联

e. 钓鱼网站 -> 后台扫描、XSS盲打

f. 木马文件 -> 同源样本关联 -> 敏感字符串特征检测

Blue Team

更多

a. Windows/Linux入侵排查思路

b. 挖矿病毒判断，中了挖矿病毒会有哪些特征？

c. 是否有日志分析经验，如果拿到一个比较大的日志文件，应该如何分析处理？

d. 在告警日志分析过程中，能否辨别常见漏洞的攻击特征？它们有哪些特点？

e. Windows/Linux环境下的抓包工具有哪些？是否掌握基本的抓包分析手法？

THANK

“交个朋友”