2022 护网面试题总结

提示：以下是本篇文章正文内容，下面案例仅供参考

一、描述外网打点的流程?

靶标确认、信息收集、漏洞探测、漏洞利用、权限获取。最终的目的是获取靶标的系统权限/关键数据。在这个过程中，信息收集最为重要。掌握靶标情报越多，后续就会有更多的攻击方式去打点。比如：钓鱼邮件、web 漏洞、边界网络设备漏洞、弱口令等。

小问题：什么是钓鱼网站?

网络钓鱼攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、帐户用户名和口令等内容。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信的站点，在所有接触诈骗信息的用户中，有高达 5%的人都会对这些骗局做出响应 。

所用的工具：

- **Wappalyzer ：** 网站技术识别工具
- **Goby/FOFA：** 网络安全测试工具，由赵武打造，它能对一个目标企业梳理最全的攻击面信息，能够快速的从一个验证入口点，切换到横向。FOFA（网络空间资产搜索引擎）
- **Masscan：** 端口扫描

二、举几个 FOFA 在外网打点过程中的使用小技巧?

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’ &&host= ‘x.cn’

框架特征：body= ‘icon-spring-boot-admin.svg’

漏洞：body= ‘index/of’ 「列目录漏洞」

三、如何识别 CND?

1、通过 ping 命令，查看回显情况

2、windows 系统环境下，使用 nslookup 进行查询，看返回的域名解析的情况

3、超级 ping 工具，比如”all-tool.cn/tools

/ping “「看 ip 结果」

四、邮件钓鱼的准备工作有哪些?

钓鱼邮件，即一种伪造邮件，是指利用伪装的电子邮件，来欺骗收件人点击恶意 URL，或诱导收件人下载带恶意程序的可执行文件。

1、确定邮件钓鱼的形式：链接、文件

2、收集目标相关的邮箱

3、编写钓鱼邮件文案

4、匿名邮箱

5、木马免杀测试、钓鱼站点搭建

6、反溯源

五、判断出靶标的 CMS，对外网打点有什么意义?

CMS 是 Content Management System 的缩写，意为“内容管理系统”。

CMS 其实是一个很广泛的称呼，从一般的博客程序，新闻发布程序，到综合性的网站管理程序都可以被称为内容管理系统。

1、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

2、根据 CMS 特征关联同 CMS 框架站点，进行敏感备份文件扫描，有可能获得站点备份文件。尝试从 CMS 源码进行代码审计，挖掘潜在漏洞。

注:

0-day，就是只有你知道的一个漏洞!

1-day，就是刚刚公布的漏洞（没有超过一天）。

n-day，就是这个漏洞已经公布出来了 N 天啦!

六、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，可向服务器发送恶意的数据，触发 log4j2 组件的缺陷，实现目标服务器的任意代码执行，获得目标服务器权限。

七、水坑攻击和鱼叉攻击的区别是什么?

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

鱼叉攻击是指利用木马程序作为电子邮件的附件，发送到目标电脑，诱导受害者去打开附件感染木马。

八、如何判断靶标站点是 windows/linux?

1、大小写检测：windows 大小写不敏感，而 linux 大小写敏感。

2、PING 指令：根据 TTL 值，winodws 一般情况下>100,linux<100

TTL(生存时间值)：该字段指定 IP 包被路由器丢弃之前允许通过的最大网段数量。

九、无法连接服务器 3389 端口的几种情况?

1、3389 端口处于关闭状态

2、远程桌面默认端口号被修改

3、防火墙=拦截

4、处于内网环境

5、超过了服务器最大的连接数

6、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。

（3389 端口是 Windows 2000(2003) Server 远程桌面的服务端口，可以通过这个端口，用"远程桌面"等连接工具来连接到远程的服务器，如果连接上了，输入系统管理员的用户名和密码后，将变得可以像操作本机一样操作远程的电脑，因此远程服务器一般都将这个端口修改数值或者关闭。）

十、如何建立隐藏用户?

1、 net user test$ 123456 /add [建立隐藏用户]

2、 net localgroup administrators test$ /add

十一、为什么 Mysql 数据库的站点，无法连接?

1、站库分离

2、3306 端口未对外开放 （3306 是 Mysql 默认端口）

3、Mysql 默认端口被修改

十二、文件上传功能的监测点有哪些?

1、客户端 Javascript 检测（文件后缀名检测）

2、服务端检测（MINE 类型检测、文件后缀名、文件格式头）

MIME（多用途互联网邮件扩展类型）

服务端 MIME 类型检测是通过检查 http 包的 Content-Type 字段中的值来判断上传文件是否合法的。

十三、常见的未授权访问漏洞有哪些?

（未授权访问漏洞可以理解为需要安全配置或权限认证的地址、授权页面存在缺陷导致其他用户可以直接访问从而引发重要权限可被操作、数据库或网站目录等敏感信息泄露。）

1、MonggoDB 未授权访问漏洞

2、redis 未授权访问漏洞

3、memcached 未授权访问漏洞

4、JOSS 未授权访问漏洞

5、VNC 未授权访问漏洞

6、Docker 未授权访问漏洞

7、Zookeeper 未授权访问漏洞

8、Rsync 未授权访问漏洞

十四、代码执行、文件读取、命令执行的函数有哪些?

文件执行：eval、call_user_func、call_user_array 等

文件读取：fopen()、readfile()、fread()、file()等

命令执行：system()、exec()、shell_exec()、passthru()、pcntl_exec()等

十五、正向 shell 和反向 shell 的区别是什么?

正向 shell：攻击者连接被攻击机器，可用于攻击者处于内网，被攻击者处于公网（外网）

反向 shell：被攻击者主动连接攻击者，可用于攻击者处于外网，被攻击者在内网。

十六、正向代理和反向代理的区别?

正向代理：当客户端无法访问外部资源的时候（谷歌、百度），可以通过一个正向代理去简洁的访问。正向代理就是处于客户端和原始服务器之间的服务器，为了从原始服务器转交请求并制定目标，客户端向代理发送请求并制定目标，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：反向代理正好相反。对于客户端来说，反向代理就好像目标服务器。并且客户端不需要进行任何设置。客户端向反向代理发送请求，接着反向代理判断请求走向何处，并将请求转交给客户端，使得这些内容就好似他自己一样，一次客户端并不会感知到反向代理后面的服务，也因此不需要客户端做任何设置，只需要把反向代理服务器当成真正的服务器就好了。

正向代理是代理客户端，为客户端收发请求，使真实客户端对服务器不可见；

而反向代理是代理服务器端，为服务器收发请求，使真实服务器对客户端不可见。

十七、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

十八、SQL 注入的种类有哪些?

1、按照注入点类型分为：数字型、字符串、搜索型

2、按照提交方式分为：post 型、get 型、cookie 型、http 头

3、按照执行结果分为：基于报错、基于布尔盲注、基于时间盲注

十九、常见的中间件有哪些？他们有那些漏洞?

1、IIS:远程代码执行、解析漏洞

2、apache：解析漏洞，目录遍历

3、Nginx：文件解析、目录遍历、目录穿越

4、JBOSS：反序列化漏洞、war 后门文件部署

5、weblogic：反序列化漏洞、SSRF 任意文件上传

二十、常见的目录扫描工具有哪些?

御剑

Dirsearch
dirmap
webdirscan

二十一、windows 常见的提权方法有哪些?

1、系统内核溢出漏洞提权

2、数据库提权

3、错误的系统配置提权

4、web 中间件漏洞提权

5、第三方软件提权

二十二、蚁剑/菜刀/C 刀/冰蝎的相同与不相同之处

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。

二十三、windows 环境下有哪些下载文件的命令?

1、certutil -urlcache -split -f

2、bitsadmin 「url」 存放路径

3、powershell 存放路径

二十四、常见的端口号？攻击点?

ftp：20、21:攻击点：匿名上传下载、嗅探、爆破

ssh：22 爆破

telent：23 攻击点：嗅探、爆破

1433 ： sql server 攻击点：注入、弱口令、爆破

1521:orcel 数据库 攻击点：注入、弱口令、爆破

7001:weblogic 中间件管理 攻击：java 反序列化、弱口令

6379:redis 数据库 攻击：未经授权、弱口令爆破

8080:JBOSS、tomcat 攻击：反序列化、控制台弱口令

8069:zabbix 攻击：远程执行、sql 注入

二十五、木马驻留系统的方式有哪些?

1、注册表

2、计划任务

3、服务

4、启动目录

5、关联文件类型

二十六、常用的威胁情报平台有哪些?

安恒威胁情报中心

奇安信威胁情报中心

绿盟威胁情报中心等。

二十七、常用的 webshell 检测工具有哪些?

1、a 盾

2、河马 webshell

3、百度 webdir

4、深信服 webshell

二十八、一般情况下。那些漏洞会被高频被用于打点?

1、阿帕奇 shiro 相关漏洞

2、log4j

3、上传漏洞

4、边界网络设备资产+弱口令

5、fastjson 漏洞

二十九、windows 常用的命令?

type：显示文件类型

dir：显示当前目录

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

三十、应急响应的基本思路是什么?

准备-检测-抑制-根除-恢复-书写报告

1、准备工作，收集信息：收集告警信息、客户反馈信息、设备主机信息等。

2、检测，判断类型：安全事件类型的判断（钓鱼邮件，webshell，爆破，中毒等）

3、抑制，控制范围，隔离失陷设备

4、根除，分析研判，将收集的信息分析

5、恢复，处置事件类型（进程、文件、邮件、启动项，注册表等）

6、输出报告

三十一、Linux 常用的命令?

cat ： 显示文件内容

ls：列出当前目录的内容

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：检测网站连接情况

crontal：检查定时任务

三十二、蓝队常用的反制手段有哪些?

1、蜜罐（蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。）

2、对攻击目标进行反渗透（IP 定位、IP 端口扫描、web 站点扫描）

3、应用漏洞挖掘&利用（菜刀、Goby、蚁剑）

4、id----> 社交特征关联

5、钓鱼网站–>后台扫描、xss 盲打

6、木马文件—>同源样本关联---->敏感字符串特侦检测

(反钓鱼也逐渐被蓝队重视，通过在服务器上故意放置钓鱼文件，吸引红队主动下载安装，完成反钓鱼。)