**渗透测试面试题**

1. **拿到一个待检测的站或给你一个网站，在已拿到授权的前提下，你会怎么做？（重点）**

**a、信息收集**

1. 首先获取到域名信息后，通过查询域名的whois信息，看是否能获取到注册者邮箱姓名电话等信息，放入社工库看是否存在密码泄露，可以通过泄露的密码进行后台登录，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. 通过域名信息查找域名所属的公司信息，通过企查查和爱企查，查找到公司信息，收集该公司人员邮箱电话信息，微信公众号，qq群，谷歌语法找相关pdf，xlsx查看工号，姓名，公开笔记（语雀等），利用该公司的信息生成专用的密码字典，方便后续的后台登录尝试和越权漏洞尝试
3. 查询服务器的旁站和子域名站点，一般主站的防护性比较完善，所有看看旁站和子域名下是否有通用性的cms或者其他信息泄露等漏洞
4. 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
5. 查看服务器的提供商，各类的云，各类的waf，vpn的设备是什么，现在的供应链是新的一个渗透方向

(供应链是什么？

供应链攻击也称为第三方攻击或后门漏洞，当黑客通过向该组织提供软件服务的第三方合作伙伴或供应商渗透企业系统时，就会发生供应链攻击。它被称为供应链攻击，因为攻击发生的漏洞点是软件供应链，比如说是

1. 奇安信vpn存在未授权管理用户遍历及任意账号密码修改
2. log4j2核弹级别漏洞，针对的是开源日志组件Apache的漏洞等
3. 阿里云如果存在漏洞，假如该站点是通过阿里云搭建的，通过阿里云漏洞就可以拿下整个网站)
4. 查询网站的真实IP地址，首先判断该网站是否存在cdn、waf，如果存在cdn，绕过cdn找到网站的真实IP地址，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. cdn回答就是cdn如何绕过方法
6. waf的话通过一个叫wafwOOf的python脚本识别，然后再针对绕过
7. 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 、google hack 进一步探测网站的信息，后台，敏感文件。

8、敏感信息收集，如 github 源码、用 7kb、破壳扫源代码泄露（.hg、.git、cvs、svn、.DS\_store源代码泄露）、google hack、接口信息泄露、社工信息泄露、邮箱地址信息收集、网盘搜索、钟馗之眼、天眼查、威胁情报、微步在线等

**b、漏洞扫描**

用 AWVS、APPSCAN、nessus等扫描器检测 Web 漏洞，如 XSS,XSRF,sql注入，代码执行，命令执行，越权访问，目录读取，任意文件读取，下载，文件包含， 远程命令执行，弱口令，上传，编辑器漏洞，暴力破解等

**c、漏洞利用**

利用以上的方式拿到 webshell，或者其他权限

**d、权限提升**

提权服务器，比如 windows 下 mysql 的 udf 提权，serv-u 提权，windows 低版本的漏洞，

如 iis6,pr,巴西烤肉，linux 脏牛漏洞，linux 内核版本漏洞提权，linux 下的 mysql system 提权以及 oracle 低权限提权

**e、日志清理**

操作系统、中间件、数据库等日志进行清除

**f、总结报告及修复方案**

整理渗透测试过程，发现漏洞过程、利用漏洞过程、漏洞是怎么产生的以及漏洞的修复方式。

**二、渗透测试过程中，都进行哪些信息收集（重点）**

1. 服务器的相关信息（真实ip，系统类型，版本，开放端口，WAF等）
2. 网站指纹识别（包括，cms，cdn，证书等），dns记录
3. whois信息，姓名，备案，邮箱，电话反查（邮箱丢社工库，社工准备等）
4. 子域名收集，旁站，C段等
5. google hacking针对化搜索，pdf文件，中间件版本，弱口令扫描等
6. 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
7. 传输协议，通用漏洞，exp，github源码等

**三、什么是cdn，如何检测cdn，如何绕过cdn（重点）**

**什么是cdn**

CDN的全称是Content Delivery Network，即内容分发网络。CDN是构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。CDN的关键技术主要有内容存储和分发技术。

其原理如下：某些大型网站在全国都会有很多用户，这些用户常常会向网站发送不同的请求，那么不同地域会具有不同的缓冲服务器来接收用户发送的流量。如果用户发送流量没有任何交互的数据，只是请求首页的话，此时根据用户所在地区来确定访问的高速缓存服务器，高速缓存服务器会返回对应的响应到用户的浏览器当中，比如广东。

CDN的优势：隐藏源主机IP，降低延迟，提高服务响应速度，增加网络冗余，减小主机服务器压力。只有当用户填写数据，需要交互时才会将请求发送到真实的服务器；此时通过广东省的缓存服务器来连接真实服务器。CDN通常存在用户很多的大型流量网站，通过它来解决服务器的瓶颈。

**验证目标是否存在挂载CDN**：

* 多地ping，查看IP是否一样；
* IP反查域名；
* nslookup查询；
* 在线IP查询 <http://tool.chinaz.com/nslookup>

**CDN绕过**

* 内部邮箱源：收集到内部邮箱服务器IP地址
* 网站phpinfo文件：phpinfo.php
* 分站IP地址，查询子域名：CDN很贵，很有可能分站就不再使用CDN
* App、小程序查询，如果目标网络站有自己的App 可以尝试通过利用fiddler或Burp Suite抓取App的请求，从里面找到目标的真实ip。
* 国外访问：<https://asm.ca.com/en/ping.php>
* 查询域名解析记录：<https://viewdns.info/>
* 网络空间引擎搜索法，常见的shodan，fofa，ZoomEye搜索。以fofa为例，只需输入：host=”XXX.com“就可以找出fofa收录的有这些关键字的ip域名，有时能获取网站的真实ip。

通过上面的方法获取了很多的IP地址，此时利用IP地址对Web站点进行访问，如果正常则说明是真实IP，否则为假。

**四、旁站和C段的区别（重点）**

旁站：同服务器其他站点；

C段：同一网段其他服务器，主站防护较强，转变目标到该站点的旁站。拿旁站权限，提权拿服务器权限。主站权限自然拿到；网站不存在旁站，进行C段探测（有些网站买断了相邻的几个IP做为分站，如果拿到分站的管理员敏感信息，如密码之类的，可以尝试对主站进行撞库）

**五、敏感信息收集都收集哪些信息（重点）**

* 后台目录：弱口令，万能密码，爆破；
* 安装包：获取数据库信息，甚至是网站源码；
* 上传目录：截断、上传图片马等；
* mysql管理接口：弱口令、爆破，万能密码；
* 安装页面 ：可以二次安装进而绕过；
* phpinfo：配置信息暴露出来；
* 编辑器：fck、kind、等
* robots.txt文件；crossdomain.xml；sitemap.xml；xx.tar.gz；xx.bak
* 源码泄露、GitHub信息泄露、社工信息泄露、邮箱信息泄露
* 相关网站查询公开信息

**六、常见的网站服务器有哪些（中间件）（重点）**

IIS、Apache、nginx、Tomcat、Weblogic、Jboss、Lighttpd

（Lighttpd是一个轻量级的Web 服务器，支持FastCGI, CGI, Auth, 输出压缩(output compress), URL重写, Alias等重要功能。它具有非常低的内存开销，cpu占用率低，效能好，以及丰富的模块等特点。其静态文件的响应能力远高于Apache，可谓Web服务器的后期之秀。）

1. **判断出网站的 CMS 对渗透有什么意义？（重点）**

1.漏洞利用：不同的CMS可能存在各种已知的漏洞和安全问题。通过了解目标网站所使用的CMS，渗透测试人员可以针对该CMS的特定漏洞进行深入研究和开发攻击脚本。这样做可以提高成功渗透的机会。

2.信息收集：CMS的版本信息以及插件、主题等扩展的存在与否都可能成为渗透测试的关键信息。确定网站使用的CMS有助于收集更准确的目标信息，并为后续测试活动提供更多的线索。

3.自动化工具选择：根据CMS的类型，可以选择特定的自动化渗透测试工具来加速测试过程。一些工具专门针对特定CMS设计，可以自动识别和利用其中的漏洞，有效地进行批量测试。

4、cms搭建的网站,可以通过指纹识别后,直接去百度搜索已经曝光的方法打一波nday ,例如：

wordpress后台修改模板拿webshell

phpmyadmin mysql log日志写shell

dedecms织梦通过文件管理器上传webshell

Drupal 存在SQL 注入漏洞

**八、Burpsuite和wireshark的区别？**

Burpsuite在抓包上侧重请求和响应的数据、Wireshark侧重于数据帧

BP http/https包、wireshark 全流量包

都是最常用一些网络抓包的工具，它们都是基于网络协议来进行嗅探信息的。不同的是，wireshark是基于较大范围的网络信息的抓取，而且他侧重于数据的整理，而burpsuite则是较有针对性的信息攻击，他的数据报文修改比较适合在网络传输中进行渗透的操作。

**九、一个成熟并且相对安全的 CMS，渗透时扫目录的意义？**

敏感文件、二级目录扫描，站长的误操作等，比如：网站备份的压缩文件、说明.txt、二级目录可能存放着其他站点。

**十、在渗透过程中，收集目标站注册人邮箱对我们有什么价值？**

* 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。
* 观察管理员常逛哪些非大众性网站，拿下它，你会得到更多好东西。

**十一、你平时常去那些网站进行学习、挖漏洞提交到那些平台**

一般去 seebug、freebuf、吾爱破解、看雪论坛、阿里聚安全、PentesterLab、阿里云先知社区、四叶草安全等。

挖洞一般提交给 360 补天、cnvd、教育漏洞平台、漏洞银行、wooyun、漏洞盒子众测平台。

**十二、你经常使用哪些工具来进行渗透测试（重点）**

web漏扫：awvs、appscan、nessus

系统扫描：nessus、nmap

目录扫描：御剑、dirb

子域名扫描：Layer、7kbscan

漏洞利用：sqlmap、beef

webshell管理工具：菜刀、蚁剑、冰蝎、哥斯拉

其他工具：Wireshark、burpsuite

**十三、burpsuite都有哪些模块**

主要模块介绍:

HTTP代理— 它作为一个 Web 代理服务器运行，并且位于浏览器和目标 Web 服务器之间。这允许拦截、检查和修改在两个方向上通过的原始流量。

Scanner(扫描器)— 一个 Web 应用程序安全扫描器，用于执行 Web 应用程序的自动漏洞扫描。

Intruder(入侵)— 此工具可以对 Web 应用程序执行自动攻击。该工具提供了一种可配置的算法，可以生成恶意 HTTP 请求。Intruder 工具可以测试和检测 SQL 注入、跨站脚本、参数篡改和易受蛮力攻击的漏洞。

Spider(蜘蛛)— 一个自动抓取 Web 应用程序的工具。

Repeater(中继器)— 一个可以用来手动测试应用程序的简单工具。它可以用于修改对服务器的请求，重新发送它们并观察结果。

Decoder(解码器)— 一种将已编码的数据转换为其规范形式，或将原始数据转换为各种编码和散列形式的工具。它能够利用启发式技术智能识别多种编码格式。

Comparer(比较)— 在任意两个数据项之间执行比较（一个可视化的“差异”）的工具。

Extender(扩展)— 允许安全测试人员加载 Burp 扩展，使用安全测试人员自己的或第三方代码扩展 Burp 的功能

Sequencer(会话)— 一种分析数据项样本随机性的工具。它可以用于测试应用程序的会话令牌或其他重要的数据项，如反 CSRF 令牌、密码重置令牌等。

**十四、NMAP的主要功能有哪些、扫描的几种方式、绕过ping扫描。（重点）**

nmap的主要功能有：主机发现（参数 -sn）、端口扫描（-sT、-sU）、版本侦测（-sV）、操作系统侦测（-O）

**nmap扫描基本场景**

1、使用TCP SYN发现活跃主机

nmap -PS 192.168.1.0/24

2、使用TCP方式扫描端口

nmap -sS -sV -n -p1-65535 -oX tcp.xml 192.168.1.0/24

3、使用UDP方式扫描端口

nmap -sS -sU -n -p1-65535 -oX udp.xml 192.168.1.0/24

4、判断操作系统

nmap -O 192.168.1.0/24

5、判断服务版本

nmap -sV 192.168.1.0/24

**扫描方式**

**-sT：**TCP connect()扫描，这是最基本的TCP扫描方式。connect()是一种系统调用，由操作系统提供，用来打开一个连接。如果目标端口有程序监听， connect()就会成功返回，否则这个端口是不可达的。这项技术最大的优点是，你勿需root权限。任何UNIX用户都可以自由使用这个系统调用。这种扫描很容易被检测到，在目标主机的日志中会记录大批的连接请求以及错误信息。

**-sS：**TCP同步扫描(TCP SYN)，因为不必全部打开一个TCP连接，所以这项技术通常称为半开扫描(half-open)。你可以发出一个TCP同步包(SYN)，然后等待回应。如果对方返回SYN|ACK(响应)包就表示目标端口正在监听；如果返回RST数据包，就表示目标端口没有监听程序；如果收到一个SYN|ACK包，源主机就会马上发出一个RST(复位)数据包断开和目标主机的连接，这实际上有我们的操作系统内核自动完成的。这项技术最大的好处是，很少有系统能够把这记入系统日志。不过，你需要root权限来定制SYN数据包。

**-sU：**UDP扫描，发送0字节UDP包，快速扫描Windows的UDP端口如果你想知道在某台主机上提供哪些UDP(用户数据报协议,RFC768)服务，可以使用这种扫描方法。nmap首先向目标主机的每个端口发出一个0字节的UDP包，如果我们收到端口不可达的ICMP消息，端口就是关闭的，否则我们就假设它是打开的。

**-sP：**ping扫描，有时你只是想知道此时网络上哪些主机正在运行。通过向你指定的网络内的每个IP地址发送ICMP echo请求数据包，nmap就可以完成这项任务。注意，nmap在任何情况下都会进行ping扫描，只有目标主机处于运行状态，才会进行后续的扫描。如果你只是想知道目标主机是否运行，而不想进行其它扫描，才会用到这个选项。

**-sA：**ACK扫描 TCP ACK扫描，当防火墙开启时，查看防火墙有未过虑某端口，这项高级的扫描方法通常用来穿过防火墙的规则集。通常情况下，这有助于确定一个防火墙是功能比较完善的或者是一个简单的包过滤程序，只是阻塞进入的SYN包。这种扫描是向特定的端口发送ACK包(使用随机的应答/序列号)。如果返回一个RST包，这个端口就标记为unfiltered状态。如果什么都没有返回，或者返回一个不可达ICMP消息，这个端口就归入filtered类。注意，nmap通常不输出unfiltered的端口，所以在输出中通常不显示所有被探测的端口。显然，这种扫描方式不能找出处于打开状态的端口。

**绕过ping扫描**

**-P0：**nmap扫描前不Ping目标主机。在扫描之前，不必ping主机。有些网络的防火墙不允许ICMP echo请求穿过，使用这个选项可以对这些网络进行扫描。

nmap -P0 192.168.1.0/24

**扫描结果端口状态说明**

* open：目标端口开启。
* closed：目标端口关闭。
* filtered：通常被防火墙拦截，无法判断目标端口开启与否。
* unfiltered：目标端口可以访问，但无法判断开启与否。
* open | filtered：无法确定端口是开启还是filtered。
* closed | filtered：无法确定端口是关闭还是filtered。

**十五、常用的端口都有哪些漏洞**

| **端口号** | **服务** | **弱点** |
| --- | --- | --- |
| 21 | FTP | 匿名上传、下载，弱口令爆破 |
| 22 | SSH | 弱口令爆破，SSH隧道及内网代理转发，文件传输 |
| 23 | Telnet | 弱口令爆破，嗅探 |
| 25 | SMTP | 邮件伪造 |
| 53 | DNS域名系统 | 允许区域传送、DNS劫持、缓存投毒、欺骗 |
| 67,68 | DHCP | DHCP劫持、欺骗 |
| 80-90 | WEB | 常见web漏洞以及是否为一些管理后台 |
| 110 | POP3协议 | 爆破、嗅探 |
| 111 | NFS | 是否匿名访问 |
| 139 | Samba服务 | 爆破、未授权访问、远程代码执行 |
| 143 | IMAP协议 | 爆破 |
| 161 | SNMP | 弱口令爆破、搜集目标内网信息 |
| 389 | LDAP目录访问协议 | 是否匿名访问，注入允许，弱口令 |
| 443 | OpenSSL | 心脏滴血以及一些web漏洞测试 |
| 445 | SMB | 弱口令爆破，检测是否有ms\_08067或者ms17\_010等漏洞 |
| 512,513,514 | Rexec | 爆破、Rlogin登陆 |
| 873,875 | Rsync | 主要看是否支持匿名，也可以跑弱口令，还有rsync 未授权访问漏洞 |
| 1025 | RPC | NFS匿名访问 |
| 1099 | JAVArmi | 远程命令执行,rmi反序列化漏洞 |
| 1352 | Lotus domino邮件服务端口 | 可能存在弱口令、信息泄露 |
| 1433 | MSSQL | 注入、提权、SA弱口令、爆破 |
| 1521 | Oracle | 弱口令爆破、TNS爆破、注入、反弹Shell |
| 1900 | bes | bes默认管理后台 |
| 2049 | NFS | 可能存在NFS配置不当 |
| 2082,2083 | cpanel主机管理系统登陆 | 弱口令爆破 |
| 2181 | ZooKeeper监听端口 | 可能存在 ZooKeeper未授权访问漏洞 |
| 2222 | DA虚拟主机管理系统登陆 | 弱口令爆破 |
| 2375 | Docker | 可能存在 Docker未授权访问漏洞 |
| 2601,2604 | zebra路由 | 默认密码zebra |
| 3128 | squid代理默认端口 | 匿名访问，可能漫游内网 |
| 3306 | MySQL | 弱口令、提权、爆破 |
| 3311,3312 | kangle主机管理系统登陆 | 说明 |
| 3389 | 远程桌面服务 | 弱口令，输入法漏洞，shirt后门，找放大镜，CVE-2019-0708 远程桌面漏洞，ms12-020 |
| 3690 | SVN | 可能存在SVN泄漏，未授权访问漏洞 |
| 4440 | rundeck | 参考漏洞: 借用新浪某服务成功漫游新浪内网 |
| 4750 | BMC | 可能存在 BMC服务器自动化RSCD代理远程代码执行(CVE-2016-1542) |
| 4848 | ClassFish | web中间件，弱口令admin/adminadmin |
| 5000 | SysBase/DB2数据库 | 可能存在爆破、注入漏洞 |
| 5432 | PostgreSQL数据库 | 弱口令爆破、注入漏洞 |
| 5560,7778 | iSqlPlus | VNC访问 |
| 5632 | PyAnywhere | 可能存在代码执行漏洞 |
| 5900,5901,5902 | VNC | 弱口令爆破，可能存在VNC未授权访问漏洞，拒绝服务攻击（CVE-2015-5239），权限提升（CVE-2013-6886） |
| 5984 | CouchDB | 可能存在 CouchDB未授权访问漏洞 |
| 6082 | varnish | 参考WooYun: Varnish HTTP accelerator CLI 未授权访问易导致网站被直接篡改或者作为代理进入内网 |
| 6379 | redis数据库 | 一般无认证，可直接访问，可能存在Redis未授权访问漏洞 |
| 6390 | Svn服务 | Svn泄露、未授权访问 |
| 7001,7002 | Weblogic | 默认弱口令，可能存在Weblogic反序列化漏洞 |
| 7778 | Kloxo | Kloxo主机控制面板登录 |
| 8000-9090 | WEB | 都是一些常见的web端口，有些运维喜欢把管理后台开在这些非80的端口上 |
| 8069 | Zabbix | 可能存在Zabbix弱口令导致的Getshell漏洞 |
| 8080 | Tomcat | 默认弱口令，Tomcat版本漏洞，低版本的utf8 directory traversal可以读取任意文件 |
| 8080,8089,9090 | JBOSS | 后台可能不认证，JBOSS版本漏洞,也可弱口令，未授权访问漏洞 |
| 8083 | Vestacp | 主机管理系统 （国外用较多） |
| 8089 | Jetty、Jenkins | 可能存在反序列化，控制台弱口令等漏洞 |
| 8161 | Apache ActiveMQ | 可能存在CVE-2016-3088漏洞，默认口令密码为：admin:admin，Apache ActiveMQ任意文件写入漏洞（CVE-2016-3088） |
| 8649 | ganglia |  |
| 8888 | amh/LuManager | 主机管理系统默认端口 |
| 9000 | fcgi | fcgi php执行 |
| 9001 | Supervisord | 可能存在Supervisord远程命令执行漏洞(CVE-2017-11610) |
| 9043/9090 | websphere | 内存泄露,可能存在WebSphere反序列化漏洞 |
| 9200/9300 | elasticsearch | 代码执行,可能存在 Elasticsearch未授权访问漏洞 |
| 9090 | WebShphere控制台 | Java反序列化、弱口令 |
| 10000 | Virtualmin/Webmin 服务器虚拟主机管理系统 | 可能存在弱口令 |
| 10001/10002 | JmxRemoteLifecycleListener | 可能存在Tomcat反序列化漏洞(CVE-2016-8735) |
| 11211 | Memcache | 未授权访问 |
| 27017,27018 | Mongodb | 未授权访问 |
| 28017 | mongodb | 统计页面 |
| 50000 | SAPManagement Console | 远程代码执行 |
| 50030,50060,50070 | HaDoop | 未授权访问 |