# 给一个IP你的渗透思路（重点）

**a、信息收集**

1、首先拿到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。

2、IP反查域名、站长之家、fofa等查询IP对应的域名信息

3、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

4、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

5、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

6、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)

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**

1、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、反序列化等。

2、用主机漏扫工具Nessus、OpenVAS、NMAP等扫描主机漏洞，查看是否存在主机漏洞，例如永恒之蓝等。

**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。

# 给一个网页你的渗透思路（重点）

1、首页查看网页的指纹信息，框架，网页开发语言信息

2、 对所有页面进行目录扫描，查找后台站点，源码、后台目录结构、通过jsfinder扫描JS敏感信息

3、 通过JS敏感信息去拼接看是否能找到接口信息，拼接接口信息看是否能找到敏感信息、未授权漏洞，拼接接口借助fuzz进行模糊探测扫描

4、检查当前网站cookie，cookie集是name=-1，将其更改为1，刷新网页

5、使用burpsuite探测网站扫描参数，抓敏感参数相关的数据包，可以借助burp插件Hae

6、找到网站后台登录地址

1. 万能密码尝试登录
2. 弱口令漏洞检测
3. BP抓包检测是否存在注入漏洞
4. 是否有不安全的信息提示，比如用户名存在，只提示密码错误，可以枚举用户名
5. 查看页面源码是否存在敏感信息泄露，如测试账户和密码
6. 不安全的验证码，验证码可以重复利用
7. 抓包查看是否存在密码明文传输
8. 登陆页面有下载app或者下载插件，可能存在任意文件下载漏洞

7、nmap 扫端口，查看端口服务开放状态。

# 3、给一个公司名称你的渗透思路（重点）

**a、信息收集**

1、通过天眼查或者企查查上先查询相关公司域名及电话、邮箱等相关信息，收集该公司所有的域名信息，可以用小蓝本，备案信息查询收集域名，收集该公司的公众号、小程序、App信息，还有该公司100%控股的公司

2、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。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），或许会找出管理员设置密码的习惯，利用该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)

6、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。

1. cdn回答就是cdn如何绕过方法
2. waf的话通过一个叫wafwOOf的python脚本识别，然后再针对绕过
3. 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。

7、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。