# 第一章 信息收集

## 一、信息收集的相关概念、作用、收集目标

渗透测试，是为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，你的公司定期更新安全策略和程序，时时给系统打补丁，并采用了[漏洞扫描器](https://baike.baidu.com/item/%E6%BC%8F%E6%B4%9E%E6%89%AB%E6%8F%8F%E5%99%A8)等工具，以确保所有补丁都已打上。如果你早已做到了这些，为什么还要请外方进行审查或渗透测试呢？因为，渗透测试能够独立地检查你的网络策略，换句话说，就是给你的系统安了一双眼睛。而且，进行这类测试的，都是寻找网络系统安全漏洞的专业人士。

### [渗透测试的8个步骤 展现一次完整的渗透测试过程及思路](http://toutiao.secjia.com/pentest-process)

发布时间：2017年10月25日 15:11    浏览量：1104

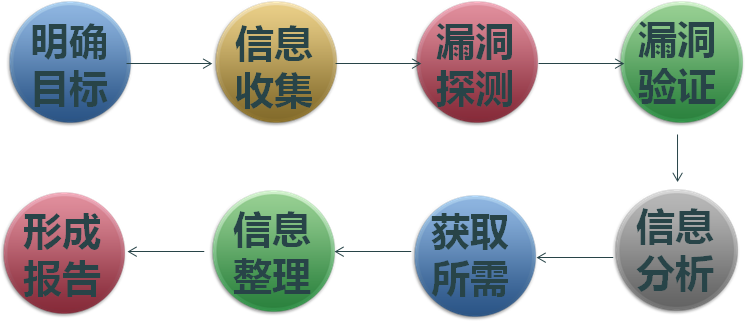
[渗透测试这个事情不是随便拿个工具就可以做了， 要了解业务还需要给出解决方案](http://toutiao.secjia.com/penetration-testing)。之前安全加介绍了金融行业 [实战微信银行渗透测试，](http://toutiao.secjia.com/weixin-bank-pentest)运营商 [渗透测试实战](http://toutiao.secjia.com/telecom-penetration-test)，今天让我们来说说 [渗透测试](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95.shtml)的流程及渗透测试相关概念。

**渗透测试流程**

**渗透测试与入侵的最大区别**

* 渗透测试：出于保护系统的目的，更全面地找出测试对象的安全隐患。
* 入侵：不择手段地（甚至是具有破坏性的）拿到系统权限。

**一般渗透测试流程**



流程并非万能，只是一个工具。思考与流程并用，结合自己经验。

**2.1 明确目标**

* 确定范围：测试目标的范围，ip，域名，内外网。
* 确定规则：能渗透到什么程度，时间？能否修改上传？能否提权等。
* 确定需求：web应用的漏洞(新上线程序)？业务逻辑漏洞（针对业务的）？人员权限管理漏洞（针对人员、权限）？等等。

（立体全方位）根据需求和自己技术能力来确定能不能做，能做多少。

**2.2 信息收集**

方式：主动扫描，开放搜索等

开放搜索：利用搜索引擎获得，后台，未授权页面，敏感url等。

* 基础信息：IP，网段，域名，端口
* 系统信息：操作系统版本
* 应用信息：各端口的应用，例如web应用，邮件应用等等
* 版本信息：所有这些探测到的东西的版本。
* 服务信息
* 人员信息：域名注册人员信息，web应用中网站发帖人的id，管理员姓名等。
* 防护信息：试着看能否探测到防护设备

**2.3 漏洞探索**

利用上一步中列出的各种系统，应用等使用相应的漏洞。方法：

* 1.漏扫，awvs，IBM appscan等。
* 2.结合漏洞去exploit-db等位置找利用。
* 3.在网上寻找验证poc。

**内容：**

* 系统漏洞：系统没有及时打补丁
* Websever漏洞：Websever配置问题
* Web应用漏洞：Web应用开发问题
* 其它端口服务漏洞：各种21/8080(st2)/7001/22/3389
* 通信安全：明文传输，token在cookie中传送等。

**2.4 漏洞验证**

将上一步中发现的有可能可以成功利用的全部漏洞都验证一遍。结合实际情况，搭建模拟环境进行试验。成功后再应用于目标中。

* 自动化验证：结合自动化扫描工具提供的结果
* 手工验证，根据公开资源进行验证
* 试验验证：自己搭建模拟环境进行验证
* 登陆猜解：有时可以尝试猜解一下登陆口的账号密码等信息
* 业务漏洞验证：如发现业务漏洞，要进行验证
* 公开资源的利用

-exploit-db/wooyun/

-google hacking

-渗透代码网站

-通用、缺省口令

-厂商的漏洞警告等等。

**2.5 信息分析**

为下一步实施渗透做准备。

* 精准打击：准备好上一步探测到的漏洞的exp，用来精准打击
* 绕过防御机制：是否有防火墙等设备，如何绕过
* 定制攻击路径：最佳工具路径，根据薄弱入口，高内网权限位置，最终目标
* 绕过检测机制：是否有检测机制，流量监控，杀毒软件，恶意代码检测等（免杀）
* 攻击代码：经过试验得来的代码，包括不限于xss代码，sql注入语句等

**2.6 获取所需**

* 实施攻击：根据前几步的结果，进行攻击
* 获取内部信息：基础设施（网络连接，vpn，路由，拓扑等）
* 进一步渗透：内网入侵，敏感目标
* 持续性存在：一般我们对客户做渗透不需要。rookit，后门，添加管理账号，驻扎手法等
* 清理痕迹：清理相关日志（访问，操作），上传文件等

**2.7 信息整理**

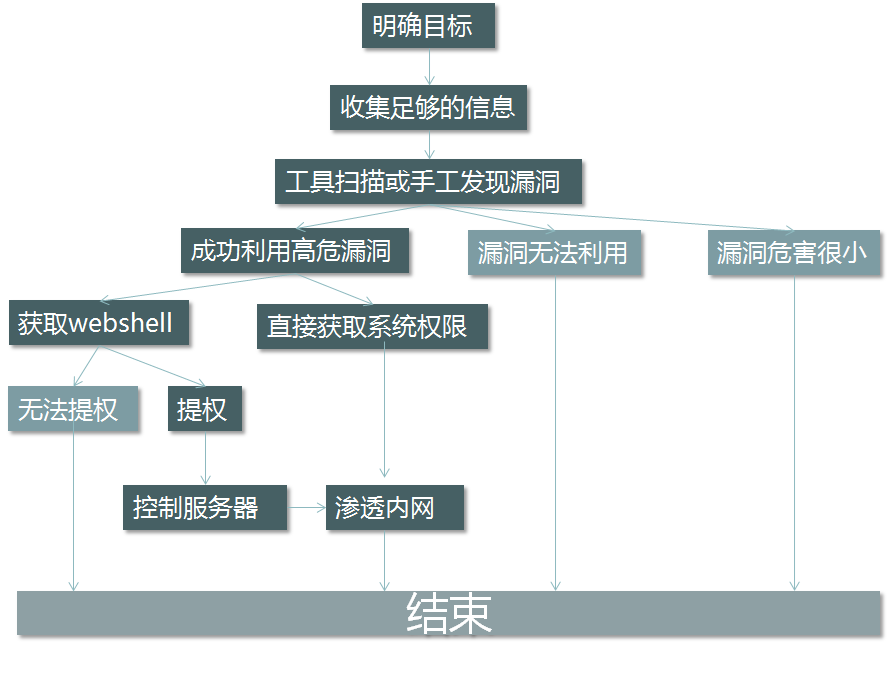
* 整理渗透工具：整理渗透过程中用到的代码，poc，exp等
* 整理收集信息：整理渗透过程中收集到的一切信息
* 整理漏洞信息：整理渗透过程中遇到的各种漏洞，各种脆弱位置信息

目的：为了最后形成报告，形成测试结果使用。

**2.8 形成报告**

* 按需整理：按照之前第一步跟客户确定好的范围，需求来整理资料，并将资料形成报告
* 补充介绍：要对漏洞成因，验证过程和带来危害进行分析
* 修补建议：当然要对所有产生的问题提出合理高效安全的解决办法

**2.9 流程总结**



**渗透测试相关名词解析**

**1.1 一些前置知识（包含但不限于）**

* 脚本（asp、php、jsp）
* html（css、js、html）
* HTTP协议
* CMS（B/S）

**1.2 肉鸡**

被黑客入侵并被长期驻扎的计算机或服务器。可以随意控制，可以是任意系统的设备，对象可以是企业，个人，政府等等所有单位。

**1.3 抓鸡**

利用使用量大的程序的漏洞，使用自动化方式获取肉鸡的行为。

**1.4 Webshell**

通过Web入侵的一种脚本工具，可以据此对网站服务进行一定程度的控制。

**1.5 漏洞**

硬件、软件、协议等等的可利用安全缺陷，可能被攻击者利用，对数据进行篡改，控制等。

**1.6 木马**

通过向服务端提交一句简短的代码，配合本地客户端实现webshell功能的木马。

<%eval request("pass")%>

<%execute(request("pass"))%>

request("pass")接收客户端提交的数据，pass为执行命令的参数值。

eval/execute    函数执行客户端命令的内容

**1.7 提权**

操作系统低权限的账户将自己提升为管理员权限使用的方法。

**1.8 后门**

黑客为了对主机进行长期的控制，在机器上种植的一段程序或留下的一个"入口"。

**1.9 跳板**

使用肉鸡IP来实施攻击其他目标，以便更好的隐藏自己的身份信息。

**1.10 旁站入侵**

即同服务器下的网站入侵，入侵之后可以通过提权跨目录等手段拿到目标网站的权限。常见的旁站查询工具有：WebRobot、御剑、明小子和web在线查询等

**1.11 C段入侵**

即同C段下服务器入侵。如目标ip为192.168.180.253 入侵192.168.180.\*的任意一台机器，然后利用一些黑客工具嗅探获取在网络上传输的各种信息。常用的工具有：在windows下有Cain，在UNIX环境下有Sniffit, Snoop, Tcpdump, Dsniff 等。

**1.12 黑盒测试**

在未授权的情况下，模拟黑客的攻击方法和思维方式，来评估计算机网络系统可能存在的安全风险。

黑盒测试不同于黑客入侵，并不等于黑站。黑盒测试考验的是综合的能力（OS、Datebase、Script、code、思路、社工）。思路与经验积累往往决定成败。

**1.13 白盒测试**

相对黑盒测试，白盒测试基本是从内部发起。白盒测试与黑盒测试恰恰相反，测试者可以通过正常渠道向被测单位取得各种资料，包括网络拓扑、员工资料甚至网站或其它程序的代码片断，也能够与单位的其它员工（销售、程序员、管理者……）进行面对面的沟通。

**1.13 黑白盒的另一种说法**

知道源代码和不知道源代码的渗透测试。这时，黑盒测试还是传统的渗透测试，而白盒测试就偏向于代码审计。

**1.14 APT攻击**

Advanced Persistent Threat，高级可持续性攻击，是指组织(特别是政府)或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。

* 1.极强的隐蔽性
* 2.潜伏期长，持续性强
* 3.目标性强

**渗透测试相关资源**

实战类：

[实战微信银行渗透测试 展示安全评估思路、工具及经验](http://toutiao.secjia.com/weixin-bank-pentest)

[某运营商渗透测试实战 展示渗透测试工具及业务系统中的常见问题](http://toutiao.secjia.com/telecom-penetration-test)

工具类：

[渗透测试人员入门 如何配置Kali Linux直接用于工作](http://toutiao.secjia.com/setup-kali-linux)

[下载 | Kali Linux2017.2新版发布 增加了一大批新网络渗透测试工具](http://toutiao.secjia.com/kali-linux-2017-2)

[安全工程师的福音 免费恶意软件分析工具FlareVM 还可进行逆向工程和渗透测试](http://toutiao.secjia.com/fireeye-releases-free-malware-analysis-toolbox)

[渗透测试工程师的17个常用工具 还有专家告诉你如何成为渗透测试人员](http://toutiao.secjia.com/17pen-testing-tools)

本文由：绿盟科技博客 发布，版权归属于原作者。   
如果转载，请注明出处及本文链接：   
<http://toutiao.secjia.com/pentest-process>  
如果此文章侵权，请留言，我们进行删除。

[全行业](http://toutiao.secjia.com/category/%E5%85%A8%E8%A1%8C%E4%B8%9A.shtml)[渗透测试](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95.shtml)[渗透测试服务](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%9C%8D%E5%8A%A1.shtml)[渗透测试工具](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E5%B7%A5%E5%85%B7.shtml)[渗透测试案例](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%A1%88%E4%BE%8B.shtml)[渗透测试方案](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%96%B9%E6%A1%88.shtml)[渗透测试步骤](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%AD%A5%E9%AA%A4.shtml)[渗透检测原理](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%A3%80%E6%B5%8B%E5%8E%9F%E7%90%86.shtml)[渗透测试概念](http://toutiao.secjia.com/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E6%A6%82%E5%BF%B5.shtml)

### PTES渗透测试执行标准

2016年11月25日 14:59:22

阅读数：3093

渗透测试注意事项：

1：不要进行恶意攻击

2：不要做傻事

3：在没有获得书面授权时，不要攻击任何目标

4：考虑你的行为将会带来的后果

5：如果你干了非法的是，天网恢恢疏而不漏

渗透测试执行标准http://www.pentest-standard.org/

1：前期交互阶段

在前期交互（Pre-Engagement Interaction）阶段，渗透测试团队与客户组织进行交互讨论，最重要的是确定渗透测试的范围、目标、限制条件以及服务合同细节。

该阶段通常涉及收集客户需求、准备测试计划、定义测试范围与边界、定义业务目标、项目管理与规划等活动。

2：情报收集阶段

在目标范围确定之后，将进入情报搜集（Information Gathering）阶段，渗透测试团队可以利用各种信息来源与搜集技术方法，尝试获取更多关于目标组织网络拓扑、系统配置与安全防御措施的信息。

渗透测试者可以使用的情报搜集方法包括公开来源信息查询、Google Hacking、社会工程学、网络踩点、扫描探测、被动监听、服务查点等。而对目标系统的情报探查能力是渗透测试者一项非常重要的技能，情报搜集是否充分在很大程度上决定了渗透测试的成败，因为如果你遗漏关键的情报信息，你将可能在后面的阶段里一无所获。

3：威胁建模阶段

在搜集到充分的情报信息之后，渗透测试团队的成员们停下敲击键盘，大家聚到一起针对获取的信息进行威胁建模（Threat Modeling）与攻击规划。这是渗透测试过程中非常重要，但很容易被忽视的一个关键点。

通过团队共同的缜密情报分析与攻击思路头脑风暴，可以从大量的信息情报中理清头绪，确定出最可行的攻击通道。

4：漏洞分析阶段

在确定出最可行的攻击通道之后，接下来需要考虑该如何取得目标系统的访问控制权，即漏洞分析（Vulnerability Analysis）阶段。

在该阶段，渗透测试者需要综合分析前几个阶段获取并汇总的情报信息，特别是安全漏洞扫描结果、服务查点信息等，通过搜索可获取的渗透代码资源，找出可以实施渗透攻击的攻击点，并在实验环境中进行验证。在该阶段，高水平的渗透测试团队还会针对攻击通道上的一些关键系统与服务进行安全漏洞探测与挖掘，期望找出可被利用的未知安全漏洞，并开发出渗透代码，从而打开攻击通道上的关键路径。

5：渗透攻击阶段

渗透攻击（Exploitation）是渗透测试过程中最具有魅力的环节。在此环节中，渗透测试团队需要利用他们所找出的目标系统安全漏洞，来真正入侵系统当中，获得访问控制权。

渗透攻击可以利用公开渠道可获取的渗透代码，但一般在实际应用场景中，渗透测试者还需要充分地考虑目标系统特性来定制渗透攻击，并需要挫败目标网络与系统中实施的安全防御措施，才能成功达成渗透目的。在黑盒测试中，渗透测试者还需要考虑对目标系统检测机制的逃逸，从而避免造成目标组织安全响应团队的警觉和发现

6：后渗透攻击阶段

后渗透攻击（Post Exploitation）是整个渗透测试过程中最能够体现渗透测试团队创造力与技术能力的环节。前面的环节可以说都是在按部就班地完成非常普遍的目标，而在这个环节中，需要渗透测试团队根据目标组织的业务经营模式、保护资产形式与安全防御计划的不同特点，自主设计出攻击目标，识别关键基础设施，并寻找客户组织最具价值和尝试安全保护的信息和资产，最终达成能够对客户组织造成最重要业务影响的攻击途径。

在不同的渗透测试场景中，这些攻击目标与途径可能是千变万化的，而设置是否准确并且可行，也取决于团队自身的创新意识、知识范畴、实际经验和技术能力。

7：报告阶段

渗透测试过程最终向客户组织提交，取得认可并成功获得合同付款的就是一份渗透测试报告（Reporting）。这份报告凝聚了之前所有阶段之中渗透测试团队所获取的关键情报信息、探测和发掘出的系统安全漏洞、成功渗透攻击的过程，以及造成业务影响后果的攻击途径，同时还要站在防御者的角度上，帮助他们分析安全防御体系中的薄弱环节、存在的问题，以及修补与升级技术方案。

渗透术语

渗透攻击（Exploit）

攻击者利用安全漏洞，所进行的攻击行为；常见的渗透攻击技术包括缓冲区溢出、web应用程序漏洞攻击（SQL注入）、利用配置错误等

攻击载荷（Payload）

目标系统在被渗透攻击之后执行的代码

shellcode

在渗透攻击时作为攻击载荷运行的一组机器指令，通常用汇编语言编写

模块（Module）

一段软件代码组件

监听器（Listener）

用来等待连入网络连接的组件

## 二、利用搜索引擎搜索信息

GoogleHacking：利用搜索引擎（如：Google，百度）有针对的搜索信息来进行网络入侵的技术和行为。搜索引擎对于搜索的关键字提供了多种语法，构造出特殊的关键字，GoogleHacking技术能够快速全面的让攻击者挖掘到有价值的信息。利用搜索引擎的搜集目标主要有一下几种：

1. 敏感信息
2. 具备特殊url关键字的目标地址
3. 搜索已有的攻击结果
4. 指定格式文件
5. 其他与某个站点相关的信息

特别提示：利用网页快照功能， 有时候可以发现很多有价值的信息

可能有人会说Google和 Google的使用方法很简单呀，写入信息，点击搜索就可以了。但实际上只是如此么？很多的以为已经被互联网删除了的文件都可以再google上面找到（快照）。

例如：在谷歌中输入 site：microsoft.com filetype：pdf，就能得到microsoft.com网站上的所有pdf文档（但是因为每个人刚学习google hacking时都是搜索这个词条，microsoft.com早已经解决了这个漏洞，所以，现在可以试试site：baidu.com filetype：pdf）

Google hacking使用的通配符：

1、加号（“+”）

“+”号是强迫包含的意思，也就是说搜索的结果中要包含后面的内容，这里需要注意的是，在“+”号前面要有一个空格，比如说我们搜索“天津 +天津特产”，搜索出的结果，一共搜索到7,750,000 条，并且都是和特产有关的。

2、减号（“—”）

减号和加号相反，就是取出的意思，他会在我们搜索结果中去除我们写入的内容、例如“天津 —特产”。

3、波浪号(“~”)

波浪号“~”的意思是搜索同义词，这样的搜索结果会更多，例如“天津 ~天津”

4、点号（“.”）

点号的作用是取代一个字符，例如“war .3”，就会搜索到4070000个结果，但是我们如果输入 war 3 则会有1310000000项结果

5、星号（“\*”）

星号的意思是取代所有字符，例如搜索“war\*”，可以搜索到1070000000项结果。

6、双引号（""）

双引号是强调的意思，例如搜索“"视界The world"”，就会搜索到93500项结果，但如果我们直接搜索“视界The world”,则时能搜索到5710项结果，就比不加双引号少了很多。

搜索引擎使用高级语法：

1、allintext

allintext的意思是以网页正文内容中的冒个字符作为搜索条件，例如“allintext：我爱你”

2、allintitle

allintitle的意思是在网页标题中搜索我们要查找的字符，例如“allintitle：视界”

3、cache

cache的意思是缓存，例如“cache：www.stuhack.com”。

4、define

define的意思是词语的定义，例如：“define：中国”

5、filetype

filetype的意思是搜索指定格式的文件，例如“filetype：MDB”，

类似于这样的搜索通常都可以直接下载，我们这样搜索很可能搜索到别人的数据口哦！

6、info

info的意思是查找指定的网站基本信息，例如：“info：www.baidu.com”。

7、link

link的意思是查看连接的网站。例如“link：www.baidu.com”

8、related

related的意思是返回主页上连接的内容，例如“related：www.baidu.com”

9、site

site的作用非常的好，它可以制定一个特定的区域进行搜索，也就是说如果site后面是一个网站，那么我们得到的内容就是关于这个网站的，例如：“site：www.baidu.com”

10、inurl

inurl的作用是搜索得到你搜索内容的网址，例如：“inurl：www.baidu.com”

上面十种用法就是在GOOGLE搜索中最常用的，希望大家能够牢记。到这里，Google hacking这节也就基本结束了，干货很多，用处也很大，但是小编还是希望大家学会这些之后多做一些有益的事情。人在做，天在看。谨记！