网站渗透测试原理及详细过程

一、简介

什么叫渗透测试?

渗透测试最简单直接的解释就是:完全站在攻击者角度对目标系统进行的安全性测试过程。

进行渗透测试的目的?

了解当前系统的安全性、了解攻击者可能利用的途径。它能够让管理人员非常直观的了解当前系统所面临的问题。为什么说叫直观呢?就像 Mitnick 书里面提到的那样,安全管理(在这里我们改一下,改成安全评估工作)需要做到面面俱到才算成功,而一位黑客(渗透测试)只要能通过一点进入系统进行破坏,他就算是很成功的了。

渗透测试是否等同于风险评估?

不是,你可以暂时理解成渗透测试属于风险评估的一部分。事实上,风险评估远比渗透测试复杂的多,它除渗透测试外还要加上资产识别,风险分析,除此之外,也还包括了人工审查以及后期的优化部分(可选)。

已经进行了安全审查,还需要渗透测试吗?

如果我对您说:嘿,中国的现有太空理论技术通过计算机演算已经能够证明中国完全有能力实现宇航员太空漫步了,没必要再发射神 8 了。您能接受吗?

渗透测试是否就是黑盒测试?

否,很多技术人员对这个问题都存在这个错误的理解。渗透测试不只是要模拟外部黑客的入侵,同时,防止内部人员的有意识(无意识)攻击也是很有必要

的。这时，安全测试人员可以被告之包括代码片段来内的有关于系统的一些信息。这时，它就满足灰盒甚至白盒测试。

渗透测试涉及哪些内容?

技术层面主要包括网络设备，主机，数据库，应用系统。另外可以考虑加入社会工程学。

渗透测试有哪些不足之处?

主要是投入高，风险高。而且必须是专业的 Ethical Hackers 才能相信输出的最终结果。

二、制定实施方案

实施方案应当由测试方与客户之间进行沟通协商。一开始测试方提供一份简单的问卷调查了解客户对测试的基本接收情况。内容包括但不限于如下：

目标系统介绍、重点保护对象及特性。

是否允许数据破坏?

是否允许阻断业务正常运行?

测试之前是否应当知会相关部门接口人?

接入方式？外网和内网?

测试是发现问题就算成功，还是尽可能的发现多的问题?

渗透过程是否需要考虑社会工程?

。。。

在得到客户反馈后，由测试方书写实施方案初稿并提交给客户，由客户进行审核。在审核完成后，客户应当对测试方进行书面委托授权。这里，两部分文档分别应当包含如下内容：

实施方案部分：

书面委托授权部分：

三、具体操作过程

3.1、信息收集过程

网络信息收集:

在这一部还不会直接对被测目标进行扫描，应当先从网络上搜索一些相关信息，包括 Google Hacking， Whois 查询， DNS 等信息（如果考虑进行社会工程学的话，这里还可以相应从邮件列表/新闻组中获取目标系统中一些边缘信息如内部员工帐号组成，身份识别方式，邮件联系地址等）。

1.使用 whois 查询目标域名的 DNS 服务器

2.nslookup

```
> set type=all

>< domain>

> server <ns server>

> set q=all

> ls -d <domain>
```

涉及的工具包括：

Google,Demon,webhosting.info,Apollo,Athena,GHDB.XML,netcraft,seologs 等等。除此之外，我想特别提醒一下使用 Googlebot/2.1 绕过一些文件的获取限制。

Google hacking 中常用的一些语法描述

1.搜索指定站点关键字 site。你可以搜索具体的站点如 site:www.nosec.org。

使用 site:nosec.org 可以搜索该域名下的所有子域名的页面。甚至可以使用 site:org.cn 来搜索中国政府部门的网站。

2.搜索在 URL 网址中的关键字 inurl。比如你想搜索带参数的站点，你可以尝试用 inurl:asp?id=

3.搜索在网页标题中的关键字 intitle。如果你想搜索一些登陆后台，你可以尝试使用 intitle:"admin login"

目标系统信息收集:

通过上面一步，我们应当可以简单的描绘出目标系统的网络结构，如公司网络所在区域，子公司 IP 地址分布，VPN 接入地址等。这里特别要注意一些比较偏门的 HOST 名称地址，如一些 backup 开头或者 temp 开关的域名很可能就是一台备份服务器，其安全性很可能做的不够。

从获取的地址列表中进行系统判断，了解其组织架构及操作系统使用情况。最常用的方法的是目标所有 IP 网段扫描。

端口/服务信息收集:

这一部分已经可以开始直接的扫描操作，涉及的工具包括：nmap,thc-amap

最常使用的参数：

nmap -sS -p1-10000 -n -P0 -oX filename.xml --open -T5 <ip address>

应用信息收集：httprint，SIPSCAN，smap

这里有必要将 SNMP 拿出来单独说一下，因为目前许多运营商、大型企业内部网络的维护台通过 SNMP 进行数据传输，大部分情况是使用了默认口令的，撑死改了 private 口令。这样，攻击者可以通过它收集到很多有效信息。snmp-gui，HiliSoft MIB Browser，mibsearch，net-snmp 都是一些很好的资源。

3.2、漏洞扫描

这一步主要针对具体系统目标进行。如通过第一步的信息收集，已经得到了目标系统的 IP 地址分布及对应的域名，并且我们已经通过一些分析过滤出少许的几个攻击目标，这时，我们就可以针对它们进行有针对性的漏洞扫描。这里有几个方面可以进行：

针对系统层面的工具有：ISS, Nessus, SSS, Retina，天镜，极光

针对 WEB 应用层面的工具有：AppScan, Acunetix Web Vulnerability Scanner, WebInspect, Nstalker

针对数据库的工具有：ShadowDatabaseScanner, NGSSQuirreL

针对 VOIP 方面的工具有：PROTOS c07 sip(在测试中直接用这个工具轰等于找死)以及 c07 h225, Sivus, sipsak 等。

事实上，每个渗透测试团队或多或少都会有自己的测试工具包，在漏洞扫描这一块针对具体应用的工具也比较个性化。

3.3、漏洞利用

有时候，通过服务/应用扫描后，我们可以跳过漏洞扫描部分，直接到漏洞利用。因为很多情况下我们根据目标服务/应用的版本就可以到一些安全网站上获取针对该目标系统的漏洞利用代码，例如 milw0rm, securityfocus,packetstormsecurity 等网站，上面都对应有搜索模块。实在没有，我们也可以尝试在 GOOGLE 上搜索“应用名称 exploit”、“应用名称 vulnerability”等关键字。

当然，大部分情况下你都可以不这么麻烦，网络中有一些工具可供我们使用，最著名的当属 metasploit 了，它是一个开源免费的漏洞利用攻击平台。其他的多

说无益，您就看它从榜上无名到冲进前五（top 100)这一点来说，也能大概了解到它的威力了。除此之外，如果您（您们公司）有足够的 moeny 用于购买商用软件的话，CORE IMPACT 是相当值得考虑的，虽然说价格很高，但是它却是被业界公认在渗透测试方面的泰山北斗，基本上测试全自动。如果您觉得还是接受不了，那么您可以去购买 CANVAS，据说有不少 0DAY，不过它跟 metasploit 一样，是需要手动进行测试的。最后还有一个需要提及一下的 Exploitation_Framework，它相当于一个漏洞利用代码管理工具，方便进行不同语言，不同平台的利用代码收集，把它也放在这里是因为它本身也维护了一个 exploit 库，大家参考着也能使用。

上面提到的是针对系统进行的，在针对 WEB 方面，注入工具有 NBSI, OWASP SQLiX, SQL Power
Injector, sqlDumper, sqlninja, sqlmap, Sqlbftools, priamos, ISR-sqlget***等等。

在针对数据库方面的工具有：

数据库 工具列表 Oracle（1521 端口）：目前主要存在以下方面的安全问题：

1、TNS 监听程序攻击（sid 信息泄露,停止服务等）

2、默认账号(default password list)

3、SQL INJECTION（这个与传统的意思还不太一样）

4、缓冲区溢出，现在比较少

了。 thc-orakel, tnscmd, oscanner, Getsids, TNSLSNR, lsnrcheck, OAT, Checkpwd, orabf MS Sql Server（1433、1434 端口） Mysql（3306 端口） DB2（523、50000、50001、50002、50003 端口）db2utils Informix（1526、1528 端口）等。

在针对 Web 服务器方面的工具有：

WEB 服务器工具列表 IIS IISPUTSCANNER Tomcat。 想起/admin 和/manager 管理目录了吗？另外，目录列表也是 Tomcat 服务器中最常见的问题。比如 5.*版本中的 http://127.0.0.1/;index.jsp

http://www.example.com/foo/"../manager/html

http://www.example.com:8080/examples/servlets/servlet/CookieExample?cookiename=HAHA&cookievalue=%5C%22FOO%3B+Expires%3DThu%2C+1+Jan+2009+00%3A00%3A01+UTC%3B+Path%3D%2F%3B

http://www.example.com:8080/servlets-examples/servlet/CookieExample?cookiename=BLOCKER&cookievalue=%5C%22A%3D%27%3B+Expires%3DThu%2C+1+Jan+2009+00%3A00%3A01+UTC%3B+Path%3D%2Fservlets-examples%2Fservlet+%3B

JBOSS 的漏洞很少，老版本中 8083 端口有%符号的漏洞：

GET %. HTTP/1.0 可以获取物理路径信息，

GET %server.policy HTTP/1.0 可以获取安全策略配置文档。

你也可以直接访问 GET %org/xxx/lib.class 来获取编译好的 java 程序，再使用一些反编译工具还原源代码。 Apache Resin http://victim/C:%5C/

http://victim/resin-doc/viewfile/?file=index.jsp

http://victim/resin-doc/viewfile/?contextpath=/otherwebapp&servletpath=&file=WEB-INF/web.xml

http://victim/resin-doc/viewfile/?contextpath=/&servletpath=&file=WEB-INF/classes/com/webapp/app/target.class

http://victim/[path]/[device].[extension]

http://victim/%20.."web-inf

http://victim/%20

http://victim/[path]/%20.xtp WebLogic

Web 安全测试主要围绕几块进行：

Information Gathering：也就是一般的信息泄漏，包括异常情况下的路径泄漏、文件归档查找等

Business logic testing：业务逻辑处理攻击，很多情况下用于进行业务绕过或者欺骗等等

Authentication Testing：有无验证码、有无次数限制等，总之就是看能不能暴力破解或者说容不容易通过认证，比较直接的就是“默认口令”或者弱口令了

Session Management Testing：会话管理攻击在 COOKIE 携带认证信息时最有效

Data Validation Testing：数据验证最好理解了，就是 SQL Injection 和 Cross Site Script 等等

目前网上能够找到许多能够用于进行 Web 测试的工具，根据不同的功能分主要有：

枚举（Enumeration）： DirBuster, http-dir-enum, wget

基于代理测试类工具：paros, webscarab, Burp Suite

针对 WebService 测试的部分有一些尚不是很成熟的工具，如：wsbang，wschess，wsmap，wsdigger，wsfuzzer

这一部分值得一提的是，很多渗透测试团队都有着自己的测试工具甚至是0DAY 代码，最常见的是 SQL 注入工具，现网开发的注入工具（如 NBSI 等）目前都是针对中小企业或者是个人站点/数据库进行的，针对大型目标系统使用的一些相对比较偏门的数据库系统（如 INFORMIX，DB2）等，基本上还不涉及或者说还不够深入。这时各渗透测试团队就开发了满足自身使用习惯的测试工具。

在针对无线环境的攻击有：WifiZoo

3.4、权限提升

在前面的一些工作中，你或许已经得到了一些控制权限，但是对于进一步攻击来说却还是不够。例如：你可能很容易的能够获取 Oracle 数据库的访问权限，或者是得到了 UNIX(AIX,HP-UX,SUNOS)的一个基本账号权限，但是当你想进行进一步的渗透测试的时候问题就来了。你发现你没有足够的权限打开一些密码存储文件、你没有办法安装一个 SNIFFER、你甚至没有权限执行一些很基本的命令。这时候你自然而然的就会想到权限提升这个途径了。

目前一些企业对于补丁管理是存在很大一部分问题的，他们可能压根就没有想过对一些服务器或者应用进行补丁更新，或者是延时更新。这时候就是渗透测试人员的好机会了。经验之谈：有一般权限的 Oracle 账号或者 AIX 账号基本上等于 root，因为这就是现实生活。

3.5、密码破解

有时候，目标系统任何方面的配置都是无懈可击的，但是并不是说就完全没办法进入。最简单的说，一个缺少密码完全策略的论证系统就等于你安装了一个不能关闭的防盗门。很多情况下，一些安全技术研究人员对此不屑一顾，但是无

数次的安全事故结果证明，往往破坏力最大的攻击起源于最小的弱点，例如弱口令、目录列表、SQL 注入绕过论证等等。所以说，对于一些专门的安全技术研究人员来说，这一块意义不大，但是对于一个 ethical hacker 来说，这一步骤是有必要而且绝大部分情况下是必须的。；）

目前比较好的网络密码暴力破解工具有：thc-hydra，brutus

>hydra.exe -L users.txt -P passwords.txt -o test.txt -s 2121 www.heimian.com ftp

目前网络中有一种资源被利用的很广泛，那就是 rainbow table 技术，说白了也就是一个 HASH 对应表，有一些网站提供了该种服务，对外宣称存储空间大于多少 G，像 rainbowcrack 更是对外宣称其数据量已经大于 1.3T。

针对网络设备的一些默认帐号，你可以查询 http://www.routerpasswords.com/和 http://www.phenoelit-us.org/dpl/dpl.html 这两个网站

3.6、进一步渗透

攻入了 DMZ 区一般情况下我们也不会获取多少用价值的信息。为了进一步巩固战果，我们需要进行进一步的内网渗透。到这一步就真的算是无所不用其及。最常用且最有效的方式就是 Sniff 抓包（可以加上 ARP 欺骗）。当然，最简单的你可以翻翻已入侵机器上的一些文件，很可能就包含了你需要的一些连接帐号。比如说你入侵了一台 Web 服务器，那么绝大部分情况下你可以在页面的代码或者某个配置文件中找到连接数据库的帐号。你也可以打开一些日志文件看一看。

除此之外，你可以直接回到第二步漏洞扫描来进行其他操作。

四、生成报告

报告中应当包含：

1.薄弱点列表清单（按照严重等级排序）

2.薄弱点详细描述（利用方法）

3.解决方法建议

4.参与人员/测试时间/内网/外网

五、测试过程中的风险及规避

在测试过程中无可避免的可能会发生很多可预见和不可预见的风险，测试方必须提供规避措施以免对系统造成重大的影响。以下一些可供参考：

1. 不执行任何可能引起业务中断的攻击（包括资源耗竭型 DoS，畸形报文攻击，数据破坏）。

2. 测试验证时间放在业务量最小的时间进行。

3. 测试执行前确保相关数据进行备份。

4. 所有测试在执行前和维护人员进行沟通确认。

5. 在测试过程中出现异常情况时立即停止测试并及时恢复系统。

6. 对原始业务系统进行一个完全的镜像环境，在镜像环境上进行渗透测试。