渗透测试技术

1 渗透测试概念

渗透测试（Penetration Test），是完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全做深入的探测，发现系统最脆弱的环节。

web 网络渗透测试：主要通过对目标系统信息的全面收集、对系统中网路设备的探测、对服务器系统主机的漏洞扫描、对应用平台及数据库系统的安全性扫描及通过应用系统程序的安全性渗透测试等手段来完成对整个 web 系统的安全性渗透检测。该渗透测试是一个完整、系统的测试过程，涵盖了网络层面、主机层面、数据层面以及应用服务层面的安全性测试。

2 渗透测试原理

渗透测试主要依据 CVE（Common Vulnerabilities & Exposures 公共漏洞和暴露）已经发现的安全漏洞，以及隐患漏洞。模拟入侵者的攻击方法对应用系统、服务器系统和网络设备进行非破坏性质的攻击性测试。

3 渗透测试目标

渗透测试利用各种安全扫描器对网站及相关服务器等设备进行非破坏性质的模拟入侵者攻击，目的是侵入系统并获取系统信息并将入侵的过程和细节总结编写成测试报告，由此确定存在的安全威胁，并能及时提醒安全管理员完善安全策略，降低安全风险。

人工渗透测试和工具扫描可以很好的互相补充。工具扫描具有很好的效率和速度，但是存在一定的误报率，不能发现高层次、复杂的安全问题；渗透测试对测试者的专业技能要求很高（渗透测试报告的价值直接依赖于测试者的专业技能），但是非常准确，可以发现逻辑性更强、更深层次的弱点。

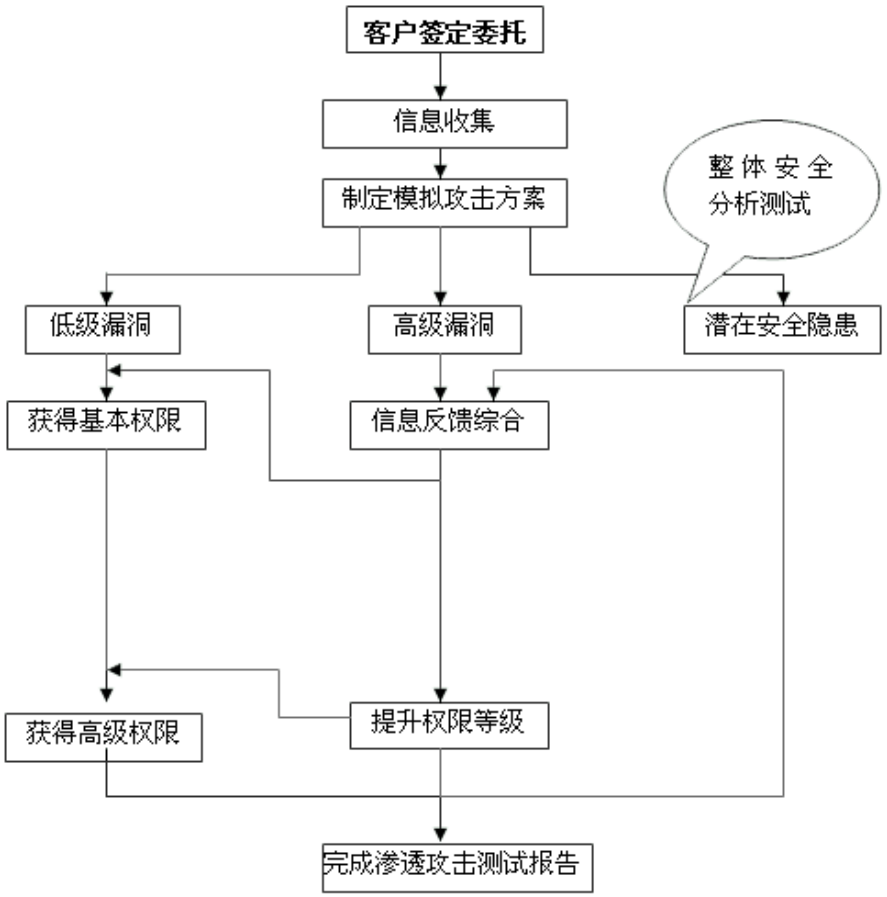
4 渗透测试特点

入侵者的攻击入侵需要利用目标网络的安全弱点，渗透测试也是同样的道理。测试人员模拟真正的入侵者入侵攻击方法，以人工渗透为主，辅助以攻击工具的使用，以保证整个渗透测试过程都在可以控制和调整的范围之内，同时确保对网络没有造成破坏性的损害。

由于采用可控制的、非破坏性质的渗透测试，因此不会对被评估的客户信息系统造成严重的影响。在渗透测试结束后，客户信息系统将基本保持一致。

5 渗透测试流程和授权

5.1 渗透测试流程



5.2 渗透测试授权

测试授权是进行渗透测试的必要条件。用户应对渗透测试所有细节和风险的知晓、所有过程都在用户的控制下进行。

6 渗透测试方法

6.1 测试方法分类

根据渗透目标分类：

1.主机操作系统渗透：

对 Windows、Solaris、AIX、Linux、SCO、SGI 等操作系统进行渗透测试。

2.数据库系统渗透：

对 MS-SQL、Oracle、MySQL、Informix、Sybase、DB2 等数据库应用系统进行渗透测试。

3.应用系统渗透：

对渗透目标提供的各种应用，如 ASP、CGI、JSP、PHP 等组成的 WWW 应用进行渗透测试。

4.网络设备渗透：

对各种防火墙、入侵检测系统、网络设备进行渗透测试。

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可能采用的技术。

5.内网测试：

内网测试指的是测试人员从内部网络发起测试，这类测试能够模拟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：远程缓冲区溢出，口令猜测，以及 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)。

6.外网测试：

外网测试指的是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。包括对网络设备的远程攻击，口令管理安全性测试，防火墙规则试探、规避，Web 及其它开放应用服务的安全性测试。

6.2 信息收集

信息收集分析几乎是所有入侵攻击的前提/前奏/基础。通过对网络信息收集分析，可以相应地、有针对性地制定模拟黑客入侵攻击的计划，以提高入侵的成功率、减小暴露或被发现的几率。

信息收集的方法包括主机网络扫描、操作类型判别、应用判别、账号扫描、配置判别等等。模拟入侵攻击常用的工具包括 Nmap、Nessus、X-Scan 等，操作系统中内置的许多工具 (例如 telnet) 也可以成为非常有效的模拟攻击入侵武器。

6.3 端口扫描

通过对目标地址的 TCP/UDP 端口扫描，确定其所开放的服务的数量和类型，这是所有渗透测试的基础。通过端口扫描，可以基本确定一个系统的基本信息，结合测试人员的经验可以确定其可能存在，以及被利用的安全弱点，为进行深层次的渗透提供依据。

6.4 权限提升

通过收集信息和分析，存在两种可能性，其一是目标系统存在重大弱点：测试人员可以直接控制目标系统，然后直接调查目标系统中的弱点分布、原因，形成最终的测试报告；其二是目标系统没有远程重大弱点，但是可以获得远程普

通权限，这时测试人员可以通过该普通权限进一步收集目标系统信息。接下来，尽最大努力获取本地权限，收集本地资料信息，寻求本地权限升级的机会。这些不停的信息收集分析、权限升级的结果将构成此次项目整个渗透测试过程的输出。

6.5 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：对网络设备和无线设备的远程攻击；对防火墙的远程攻击或规则探测、规避尝试。 信息的收集和分析伴随着每一个渗透测试步骤，每一个步骤又有三个组成部分：操作、响应和结果分析。

6.6 溢出测试

当测试人员无法直接利用帐户口令登陆系统时，也会采用系统溢出的方法直接获得系统控制权限，此方法有时会导致系统死机或从新启动，但不会导致系统数据丢失，如出现死机等故障，只要将系统从新启动并开启原有服务即可。一般情况下，如果未授权，将不会进行此项测试！

6.7 SQL 注入攻击

SQL 注入常见于应用了 SQL 数据库后端的网站服务器，入侵者通过提交某些特殊 SQL 语句，最终可能获取、篡改、控制网站服务器端数据库中的内容。此类漏洞是入侵者最常用的入侵方式之一。

6.8 检测页面隐藏字段

网站应用系统常采用隐藏字段存储信息。许多基于网站的电子商务应用程序用隐藏字段来存储商品价格、用户名、密码等敏感内容。恶意用户通过操作隐藏字段内容达到恶意交易和窃取信息等行为，是一种非常危险的漏洞。

6.9 跨站攻击

入侵者可以借助网站来攻击访问此网站的终端用户，来获得用户口令或使用站点挂马来控制客户端。

6.10WEB 应用测试

Web 脚本及应用测试专门针对 Web 及数据库服务器进行。根据最新的统计，脚本安全弱点为当前 Web 系统，尤其是存在动态内容的 Web 系统比较严重的安全弱点之一。利用脚本相关弱点轻则可以获取系统其他目录的访问权限，重则将有可能取得系统的控制权限。因此对于含有动态页面的 Web、数据库等系统，Web 脚本及应用测试将是必不可少的一个环节。在 Web 脚本及应用测试中，可能需要检查的部份包括：

1.检查应用系统架构,防止用户绕过系统直接修改数据库；

2.检查身份认证模块，用以防止非法用户绕过身份认证；

3.检查数据库接口模块，用以防止用户获取系统权限；

4.检查文件接口模块，防止用户获取系统文件；

5.检查其他安全威胁；

6.11 代码审查

对受测业务系统站点进行安全代码审查的目的是要识别出会导致安全问题和事故的不安全编码技术和漏洞。这项工作虽然可能很耗时，但是必须进行，代码审查测试工作包括如下工作但不仅限于此：

审查代码中的 XSS 脚本漏洞；

审查代码中的 SQL 注入漏洞；

审查代码中的潜在缓冲区溢出；

审查识别允许恶意用户启动攻击的不良代码技术；

其他软件编写错误及漏洞的寻找及审查。

6.12 第三方软件误配置

第三方软件的错误设置可能导致入侵者利用该漏洞构造不同类型的入侵攻击。

6.13Cookie 利用

网站应用系统常使用 cookies 机制在客户端主机上保存某些信息，例如用户 ID、口令、时戳等。入侵者可能通过篡改 cookies 内容，获取用户的账号，导致严重的后果。

6.14 后门程序检查

系统开发过程中遗留的后门和调试选项可能被入侵者所利用，导致入侵者轻易地从捷径实施攻击。

6.15VOIP 测试

在对受测网络进行渗透测试时，将会进行 VoIP 业务的安全测试，所有影响数据网络的攻击都可能会影响到 VoIP 网络,如病毒、垃圾邮件、非法侵入、DoS、劫持电话、偷听、数据嗅探等，因此，首先会对 VoIP 网络进行安全测试，接着对 VoIP 服务器进行测试，这些服务器常常是恶意攻击者的靶子,因为它们是任何一个 VoIP 网络的心脏。服务器存在的致命弱点包括其操作系统、服务及它所支持的应用软件，可能都会存在安全漏洞。要将黑客对服务器的攻击降至最小程度，就要对 VoIP 网络及其服务器、软终端进行全面的安全测试，以查找安全隐患，协助用户技术人员修补这些漏洞。

6.16 其他测试

在渗透测试中还需要借助暴力破解、网络嗅探等其他方法，目的也是为获取用户名及密码。

7 常用渗透测试工具

可能使用到的命令和工具包括：

7.1 命令：

Google 搜索和攻击；

DNS 工具：例如：Whois，nslookup, DIG 等等；

各种测试命令；

在线网络数据库：Ripe, Afrinic, APNIC, ARIN LACNIC

7.2 工具：

主流商业扫描器：ISS Internet Scanner、NEUUS、Core Impact 、NSfocus 极光扫描器.

黑客常用端口扫描器：如：NMAP、 Superscan…

SNMP Sweepers (Solarwinds)…

Website mirror tools (HTTrack, teleport pro)…

无线网络扫描工具(Netstumbler, Kissmet, Wellenreiter, Airsnort)

WEB 漏扫工具 AppScan,wvs, WebInspect, Nstalker、nikto、google hack

溢出工具：Metasploit

破解工具:John the Ripper、THC Hydra、L0phtcrack、 Aircrack、Airsnort 、Pwdump

Sniffer 工具：Wireshark、Kismet、Tcpdump 、Cain and Abel

Ettercap、NetStumbler

7.2.1 应用层工具

Acunetix Web Vulnerability Scanner（漏洞扫描工具）

这是一款网络漏洞扫描工具。通过网络爬虫测试网站安全，检测流行的攻击，如跨站点脚本、sql 注入等。在被入侵者攻击前扫描购物车、表格、安全区域和其他 Web 应用程序。

7.2.2 系统层工具

SSS6.0 扫描器汉化版

Shadow Security Scanner v6.67.58，02 月 09 日发布，俄罗斯安全界非常专业的安全漏洞扫描软件，具有安全扫描，口令检查，操作系统检查等强大功能，支持在线升级。

ISS 漏洞扫描器

ISS（国际互联网安全系统公司）是在信息安全领域中专门致力于反黑客攻击的专业公司。目前它的主要产品有四大系列：Real Secure(实时入侵监测器)、Internet Scanner(互联网扫描器)、System Scanner(系统扫描器)、Database Scanner(数据库扫描器)。其中 Real Secure 和 Internet Scanner 是其拳头产品，Database Scanner 是其独有的专用数据库防黑安全产品。

nmap 端口扫描工具

nmap 是目前为止最广为使用的国外端口扫描工具之一。它可以很容易的安装到 Windows 和 unix 操作系统中，包括 mac os x(通过 configure、make 、make install 等命令）然后对主机和网络设备进行端口扫描，以寻找目标主机的漏洞。

7.2.3 网络层工具

SolarWinds Engineer’ s Edition

是一套非常全面的网络工具库，包括了网络恢复、错误监控、性能监控和管理工具等。除了包含 Professional PLUS Edition 中所有的工具外，Engineer’s Edition 还增加了新的 Swich Port Mapper 工具，它可以 switch 上自动执行 Layer 2 和 Layer 3 恢复。此工程师版包含了 Solarwinds MIB 浏览器和网络性能监控器（Network Performance Monitor），以及其他附加网络管理工具。

7.2.4 其他方法和工具

Whois 命令——是一种 Internet 目录服务，whois 提供了在 Internet 上一台主机或者某个域的所有者信息，如管理员的姓名、地址、电话号码等，这些信息通常保存在 Internlc 的数据库内。一旦得到了 Whois 记录，从查询的结果还可以得知 primary 和 secondary 域名服务器的信息。

Nslookup——一种 DNS 的排错工具，可以使用 nslookup 命令把你的主机伪装成 secondaryDNS 服务器，如果成功便可以要求从主 DNS 服务器进行区域传送，如果传送成功，可以获得大量有用的信息。

Traceroute——用于路由追踪，判断从你的主机到目标主机经过了哪些路由器、跳计数、响应时间、路由器通断情况等，大多数的操作系统自带了自己版本的 traceroute 程序。

端口扫描程序——专用的对网络端口进行扫描的工具，定义好 IP 地址范围和端口后就可以开始扫描。

网络侦查和服务器侦查程序——通过该种程序可以侦查出网络上已经开启的端口。如 PingPro 的工作是是通过监控远程工程调用服务。

以及测试人员自行编译的渗透测试工具等等。

8 渗透测试风险规避措施

渗透测试过程中可能对业务产生影响，可以采取以下措施来减小风险：

1.在渗透测试中不使用含有拒绝服务的测试策略。

2.渗透测试时间尽量安排在业务量不大的时段或者晚上。

3.在渗透测试过程中如果出现被评估系统没有响应的情况，应当立即停止测试工作，与用户相关人员一起分析情况，在确定原因后，并待正确恢复系统，采取必要的预防措施（比如调整测试策略等）之后，才可以继续进行。

4.测试人员会与用户网站系统和安全管理人员保持良好沟通。随时协商解决出现的各种难题。

5.测试方自控：由渗透测试方对本次测透测试过程中的三方面数据进行完整记录：操作、响应、分析，最终形成完整有效的渗透测试报告提交给用户。