KNOWNSEC
知 道 创 宇

知 道 创 宇
安全服务部产品白皮书

[版本：V 1.5]

咨询电话：（010）57076191-8021

版本说明

修订人	修订内容	修订时间	版本号	审阅人
沈瑞	文档创建与编写	2016-5-30	0.1	王宇
沈瑞	文档内容修正	2016-6-20	1.0	王宇
沈瑞	新增漏洞扫描、应急响应内容	2016-9-9	1.5	王宇

文档信息

文档名称	知道创宇安全服务部产品白皮书	文档编号	KSA-TS-03
文档版本号	V1.5	保密级别	公开
扩散范围	公开		
扩散批准人			

文档说明

本文档为北京知道创宇信息技术有限公司（以下简称“知道创宇”）安全服务部产品白皮书，用于描述知道创宇高级渗透测试及专业渗透测试等服务内容、方法及相关工具等。

版权声明

目 录

1. 国内信息安全情况概述

1.1 国内信息安全环境简述

2015 年是我国“十二五”规划收官之年，我国实现了半数中国人接入互联网，网民规模达 6.88 亿，手机网民规模达 6.2 亿，域名总数为 3102 万个。2015 年，我国陆续出台了“互联网＋”行动计划、“宽带中国 2015 专项行动”等，加快建设网络强国。我国不断完善网络安全保障措施，网络安全防护水平进一步提升。然而，层出不穷的网络安全问题仍然难以避免。基础网络设备、域名系统、工业互联网等我国基础网络和关键基础设施依然面临着较大安全风险，网络安全事件多有发生。木马和僵尸网络、移动互联网恶意程序、拒绝服务攻击、网页仿冒、网页篡改等网络安全事件表现出了新的特点：利用分布式拒绝服务攻击（以下简称“DDoS 攻击”）和网页篡改获得经济利益现象普遍；个人信息泄露引发的精准网络诈骗和勒索事件增多；智能终端的漏洞风险增大；移动互联网恶意程序的传播渠道转移到网盘或广告平台等网站。

1.2 2016 年信息安全趋势预测

1.2.1 工业互联网面临的网络安全威胁加剧

2015 年，国家信息安全漏洞共享平台（以下简称“CNVD”）共收录工控漏洞 125 个，发现多个国内外工控厂商的多款产品普遍存在缓冲区溢出、缺乏访问控制机制、弱口令、目录遍历等漏洞风险，可被攻击者利用实现远程访问。据监测，2015 年境外有千余个 IP 地址对我国大量使用的某款工控系统进行渗透扫描，有数百个 IP 地址对我国互联网上暴露的工控设备进行过访问。2015 年 12 月，因遭到网络攻击，乌克兰境内近三分之一的地区发生断电事故。据分析，此次网络攻击利用了一款名为“黑暗力量”的恶意程序，获得了对发电系统的远程控制能力，导致电力系统长时间停电。此次事件的发生，再次对我国提出警示，我国工业互联网也可能面临着严峻的网络安全威胁。

1.2.2 个人信息泄露

2015 年我国发生多起危害严重的个人信息泄露事件。例如某应用商店用户信息泄露事件、约 10 万条应届高考考生信息泄露事件、酒店入住信息泄露事件、某票务系统近 600 万用户信息泄露事件等。

由于许多网民习惯在不同网站使用相同账号密码，个人隐私信息易被“撞库”等黑客行为窃取，进而威胁到网民财产安全。预计在 2016 年个人信息泄露事件数量仍呈上升趋势。

1.2.3 云平台和大数据的安全防护能力将是关注重点

随着云计算、大数据等新技术、新业务的应用与发展，更多政府和企业将系统部署到云平台，大量涉及国计民生、企业运营的数据和用户个人信息存储在云上，吸引了攻击者的目光。攻击者不断挖掘云平台自身可能存在的安全漏洞，一旦发现漏洞并加以利用，可能导致严重的大规模信息泄露事件发生。此外，攻击者也可以利用云平台实施网络攻击，例如在云平台上部署网络攻击控制端、仿冒站点或发动 DDoS 攻击等。因此，云平台和大数据的安全防护将成为行业重点关注的问题。

2. 渗透测试简介

渗透测试是完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全作深入的探测，发现系统最脆弱的环节。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。渗透测试是一种非常专业的安全服务。

APT测试

模拟高级黑客进行APT测试，协助客户抵御专业跨国黑客组织。

KSA渗透测试

发现和挖掘网站和业务系统存在的代码漏洞和逻辑漏洞。

APP渗透测试

对移动APP程序进行安全测试，防止黑客利用APP漏洞获取私利。

微信服务号渗透

对目前广泛应用的微信服务号进行安全测试。

2.1 渗透测试工作的必要性

渗透测试利用网络安全扫描器、专用安全测试工具和富有经验的安全工程师的人工经验对网络中的核心服务器及重要的网络设备，包括服务器、网络设备、防火墙等进行非破坏性质的模拟黑客攻击，目的是侵入系统并获取机密信息并将入侵的过程和细节产生报告给用户。

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和漏报率，并且不能发现高层次、复杂、并且相互关联的安全问题；渗透测试需要投入的人力资源较大、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机能及技能），但是非常准确，可以发现逻辑性更强、更深层次的弱点。

2.2 渗透测试工作的作用与收益

- 技术安全性的验证

渗透测试作为独立的安全技术服务，其主要目的就在于验证整个目标系统的技术安全性，通过渗透测试，可在技术层面定性的分析系统的安全性。

- 查找安全隐患点

渗透测试是对传统安全弱点的串联并形成路径，最终通过路径式的利用而达到模拟入侵的效果。所以，在渗透测试的整个过程中，可有效的验证每个安全隐患点的存在及其可利用程度。

- 安全教育

渗透测试的结果可作为内部安全意识的案例，在对相关的接口人员进行安全教育时使用。

- 安全技能的提升

一份专业的渗透测试报告不但可为用户提供作为案例，更可作为常见安全原理的学习参考。

2.4 渗透测试方式说明

2.4.1 自动测试

自动测试是指借助系统和应用扫描工具对站点的系统层和应用层进行全面的安全扫描，以此种方法来检测目标系统中是否包含已知的安全问题。

因自动测试的方式借助了自动化的扫描工具，因此其优点在于检测速度较快，而且对已知漏洞的检测也较为全面。而它的缺点也显而易见：

- 自动化工具对于某些特殊的信息无法实现自动甄别
- 一些复杂的客户端脚本无法完全实现自动检测
- 一些具有较强逻辑性的业务无法通过自动化工具实现检测
- 自动化工具均无法避免误报

2.4.2 手动测试

手动测试作为自动测试的一种补充，是渗透测试过程中必不可少的一个重要部分，但因手动测试由测试人员发起，因此，测试人员的个人技能和经验直接影响手动测试的结果。

一般手动测试主要涵盖以下几个方面：

- 对自动测试结果的验证

  自动化检测工具难免存在误报，因此，手动测试过程中需要筛选自动化检测结果中的误报，同时还要对正确告警的结果进行验证和再利用，以

确认其危险程度与自动扫描结果一致

- 个性化页面信息的人工甄别

  多数自动化测试工具，其检测条件都是以页面返回页面中的关键字或 HTTP 状态值作为判断条件，而某些经过精心构造的个性化页面，其返回内容可能无法完全由自动化工具进行判断，因此，针对这样的站点就需由人工进行手动测试

- JavaScript 测试

  随着 WEB2.0 的兴起，JavaScript 被很多站点大量使用，而自动化扫描工具对 JavaScript 脚本的解析能力不强，在自动扫描过程中难免遗漏，因此，手动测试中，测试人员需对那些自动化扫描工具无法解析的、含有 JavaScript 脚本的页面进行二次测试，以检测其安全性

- 提交数据的精细化测试

  自动化测试过程中，在对提交数据进行构造时，其构造方式均遵循一定的规律，而手动测试则可避免这样的问题出现，因此，某些可从本地构造恶意数据并提交测试的页面，也需在手动测试过程中进行深度测试

- 业务逻辑的安全测试

  业务逻辑相对来说与程序本身关系不大，因此，无论使用什么的自动化检测工具都无法检测业务逻辑的正确与否，所以，这部分就需要人工检测过程中，先对已有业务逻辑进行分析判断，然后再结合测试人员的经验对业务逻辑安全性进行必要的检测

由此可见，手动测试会在深度与广度两方面弥补自动化测试的不足，是保障渗透测试质量的一个重要手段，也是渗透测试的精髓所在。

2.5 渗透测试服务的独立性

如上所述，渗透测试可以作为风险评估的一部分，但它也具有独立性，换言之，渗透测试本身可以独立于风险评估而存在。

渗透测试作为独立的安全服务时，其工作内容及效果与作为风险评估中的一

部分工作并不存在明显差异，但相对整体的风险评估来说，渗透测试作为独立的一项安全服务时，其所能涵盖和涉及的内容相对较少，但相对的，其效果也更具备针对性。因此，对于迫切需要验证整体系统技术安全性而又不需要大规模风险评估的情况下，可选择渗透测试服务。

3. 渗透测试服务内容

3.1 WEB 渗透测试最佳实践

与传统操作系统的渗透测试不同，针对 WEB 应用的渗透测试没有一个可依赖的、完整的漏洞库可用于检测，因此，在测试过程中，知道创宇会以攻击方式为测试视角，对目标系统进行已知攻击方式的检测，对于已知攻击方式，包主要参考 OWASP 组织统计的 63 种常见 WEB 攻击手段，以及 WASC 的 WEB 安全威胁中 34 种 WEB 威胁。

3.2 测试方式分类

3.1.1.黑盒测试

黑盒测试愿意是指，把程序看作一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下，通过测试来检测每个功能是否都能正常使用。

在渗透测试中，黑盒测试则是指，测试人员在仅获得目标的 IP 地址或域名信息的情况下，对目标系统发起模拟入侵的尝试。

3.1.2.内部测试与外部测试

内部测试是指，测试人员在用户现场直接介入到用户内部网络，对目标系统发起模拟入侵的测试行为。内部测试主要针对以下情况：

- 需绕过边界防护设备

  被测试的目标系统置于边界防护设备之后，且边界防护设备的有效性和安全性不包含在测试要求中的情况下，可通过接入到网络内部来实现对目标系统的直接、无防护的访问，这样可有效减少在绕过防护设备时所耗费的时间和成本开销。

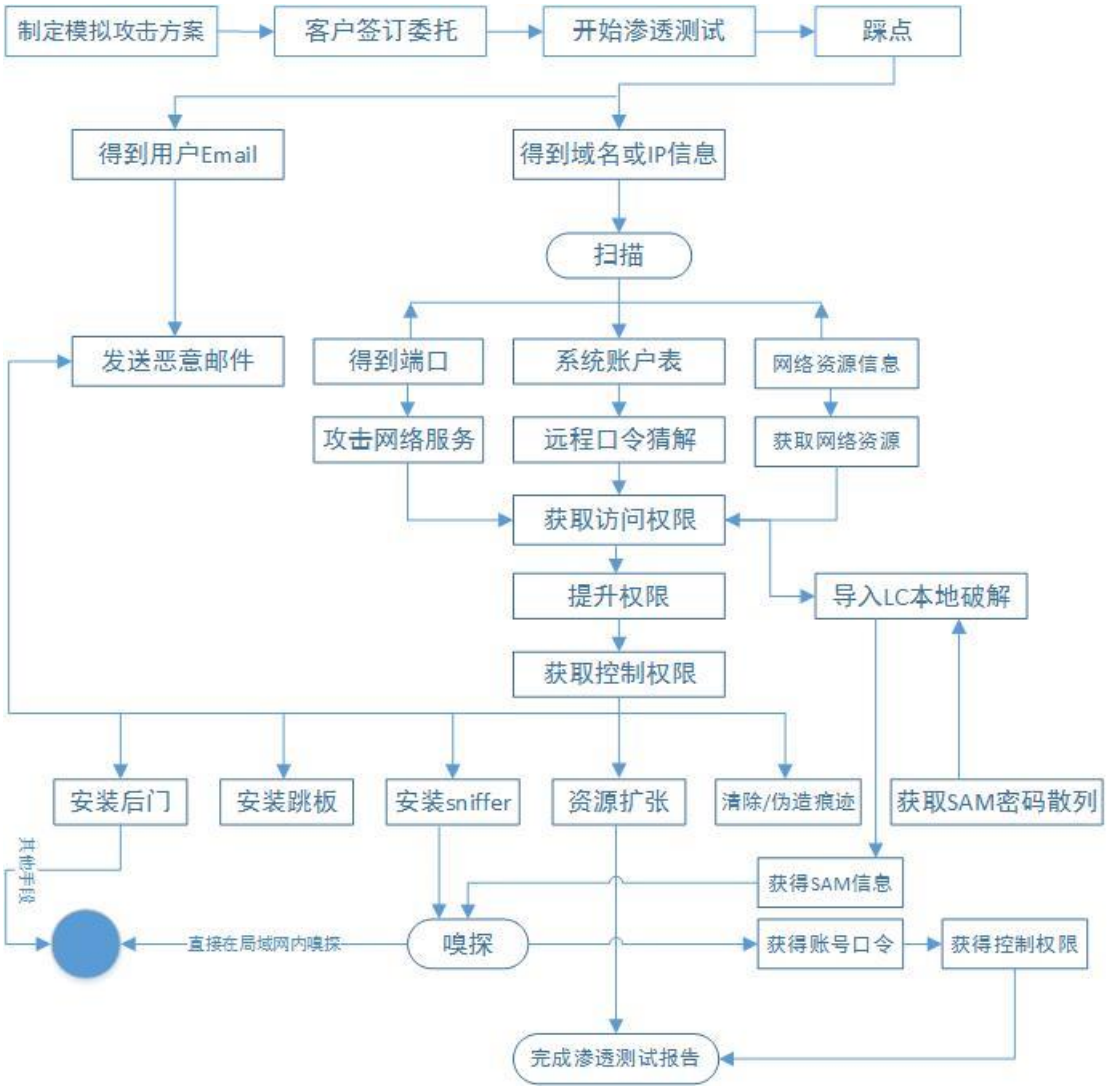
- 模拟内部入侵行为

  某些 IT 系统其设计的目的便在于服务于内部用户，而常规安全威胁中，来自企业内部的威胁并不少于外部的威胁，因此，为验证内部威胁可能对内部 IT 系统造成的伤害，内部的渗透测试也是常见的渗透测试服务的一种方式。

相对内部测试而已，外部测试则是指用户直接从互联网对测试目标系统进行访问和各类安全测试，这种测试用于验证来自互联网的威胁。

3.3 渗透测试服务流程

渗透测试的服务流程如下：



渗透测试流程图

3.3.1 实施方案制定&及时的客户交流

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。这也是高级渗透测试服务与黑客攻击入侵的本质不同。

3.3.2 目标系统信息收集&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（知道创宇 Websoc 等），免费安全检测工具（如，NMAP、NESSUS 等）。操作系统内置的许多功能（如,TELNET、NSLOOKUP、IE 等）也可以作为信息收集的有效工具。

3.3.3 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。

3.3.4 报告制作

渗透测试之后会提供一份渗透测试报告，渗透测试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。

4. Web 渗透测试检查类

4.1 信息收集

4.1.1 公开信息收集

公开信息，即是指那些暴露于网络上，不需要额外的授权便可获取到的信息，这些信息主要通过以下几个手法获取：

- nslookup 查询 DNS 记录
- whois 查询域名注册信息
- 域名反查系统查询同主机上运行的其他站点
- 利用 Google hacking 查询敏感页面

4.1.2 目标系统信息探测

目标系统信息探测主要通过端口扫描、banner 信息及指纹监测等方式进行的针对特定服务及端口的版本信息探测过程，通过这些版本信息测试人员可对目标系统进行更具有针对性的测试。

4.1.3 漏洞自动化识别

漏洞自动化识别主要是借助自动化扫描系统从系统层和应用层两个层面，对目标系统发起的漏洞检测工作，系统层面的漏洞检测主要从以下几个方面进行：

- 溢出漏洞

- 口令破解
- 信息泄露

应用层的漏洞检测主要包含以下几个方面：

- 信息泄露
- 配置错误
- 认证破解
- 注入攻击
- 跨站脚本（XSS，Cross Site Script）
- 跨站请求伪造（Cross Site Request Forgery）
- 错误的重定向
- ……

4.2 常规 Web 渗透人工检测

手工检测的过程主要有几个作用：

1、对自动化检测结果的校验与验证

2、利用测试人员的经验深度挖掘漏洞

3、利用人自身的逻辑识别能力挖掘某些逻辑错误而导致的漏洞

手工漏洞的检测与挖掘，会围绕以下几类漏洞开展：

4.2.1 信息泄露

常规自动化检测的信息泄露主要针对某些已知类型的威胁进行的，如：返回页面中包含路径信息、某目录存在匿名目录浏览、某文件存在自动备份文件等等。

但某些信息泄露漏洞往往需要人工介入判断，如，返回信息中存在与目标系统业务具有极大相关性的数据，这些数据的泄露十分危险，但却无法被机械化扫描工具所识别，所以需要人工对此类信息泄露进行挖掘和验证。

4.2.2 注入漏洞

注入漏洞分为多种注入方式，如：SQL 注入、XPath 注入、LDAP 注入等等。

不同类型的注入漏洞在利用方式和原理上是相似的，但后台存储的数据内容

和用户权限决定了注入漏洞所能获得的收益大小，因此，测试人员手动介入测试注入漏洞时，除验证注入漏洞是否真实存在外，还需对注入漏洞所产生危害的深度与广度进行识别，并结合其影响为该注入漏洞设置合理的危险等级。

4.2.3 XSS 与 CSRF 深度利用

多数 WEB 扫描器对 XSS 与 CSRF 的测试与识别方式单一，一般情况下，扫描器仅仅只能从理论层面验证这类漏洞的存在，但这类漏洞所能带来的安全风险，需由人工辅助来完成鉴别与评估。

4.2.4 重定向检测与利用

重定向漏洞往往被用来与其他漏洞相结合使用，因此，在传统的自动化评估过程中，难以对重定向漏洞进行识别和深度的利用，但通过人工检测的方式，可对重定向漏洞的利用方式及其影响进行重新评估与定义。

4.2.5 参数错误

参数错误分为多种方式，但其中很多设计到逻辑及权限错误的问题时，就难以通过扫描器实现自动识别，对这类错误，往往需要借助渗透工程师的丰富测试经验来进行识别和测试。

4.2.6 认证错误

认证错误包含多层含义，对于其最简单的理解便是用户登录入口暴露（尤其是敏感用户的登录入口，如：管理登录入口），且存在弱口令或暴力破解的可能（如：无验证码的登录页面即可通过暴力破解的方式尝试通过验证）。

而除此之外，还有某些认证错误是自动化程序无法识别的，例如，登录某系统之后，系统内的任意操作不再对用户身份进行校验，或者，当用户修改口令的时候不对原始口令进行校验，这样的漏洞都可能导致普通用户的越权行为。

4.2.7 漏洞验证

漏洞验证分为三个层面：

- 漏洞是否存在

某些漏洞是存在的，但其利用成本却较高。

如：会话破解，会话破解在理论上是可行的，但若目标系统中不存在易猜解的用户口令，则其可利用程度是相当低的，甚至可以说从实际操作上是不可利用的。

对于此类漏洞，仅具备“存在性”，因此从威胁的定量分析上，其威胁得分也相对较低。

- 漏洞是否可利用

  即，漏洞不但存在，且可利用成功。

- 漏洞利用后获得的权限

  成功后的权限决定了漏洞的危险等级，利用成功后所获得权限越高，恶意用户所产生的恶意行为危害也就越大，其危险等级也就越高。

4.3 Web 业务逻辑检测-业务逻辑

4.3.1.逻辑错误测试概述

由于逻辑错误并不涉及到程序自身的错误及异常，因此，在自动化检测过程中，逻辑错误是无法被识别的。

逻辑错误不但需要人工进行检测，而且还需要检测人员在检测之前对业务有所了解，因此，在检测前，测试人员往往会构造大量的数据进行测试，以学习业务的正常逻辑，从而进一步构造可能造成业务危害的错误逻辑数据，以达到逻辑测试的目的。

其中逻辑错误的类型有：

- 授权绕过漏洞

  业务系统中针对未加权认证、平行认证、敏感接口等缺乏认证，从而导致的越权操作及后台可猜解漏洞。

  通常对于是否存在授权绕过采用的测试方面有：

- 当用户没有通过验证时，是否有可能访问该资源？
- 是否有可能在注销后访问该资源？
- 是否有可能获得只应由拥有不同角色/特权的用户才能访问的功能和资源？
- 尝试作为管理员用户访问应用程序并追踪所有的管理职能。如果测试者用普通用户身份登录是否有可能访问这些管理职能？
- 因拥有不同权限，而导致操作被拒绝的用户是否有可能使用这些功能？

- 截获和修改金额漏洞

  由于支付业务功能缺乏针对提交方式、服务器验证返回等手段，导致的订单支付金额可修改漏洞。通常会导致重大损失。

  例如：在北加州，某电视台的网站为了 Web2.0 化，开发了一个新

的功能：允许网友们提供当地的天气信息，该信息将在电视新闻中滚动播出。为了防止垃圾信息，网友们提供的信息是经过人工审核后才播出的。

但是这套系统在设计时还允许网友们对信息进行编辑。此处存在一个逻辑漏洞：审核通过后的信息，如果被用户重新编辑了，不会再次进行审核，也会直接发送到电视新闻的滚动条中。于是不少人利用这一逻辑漏洞，在电视新闻中发送各种垃圾信息。

- 规避交易限制

类似于“截获和修改金额漏洞”，通过对会话的修改，突破交易限制。如：“某产品购买数量 100 份起，通过修改，可 1 份下单。”

例如：开发人员没有对购买的数量进行严格的限制，当购买的数量是一个负数时，总额的算法仍然是"购买数 量 x 单价=总价"，所以这样就会导致有一个负数的需支付金额。若仍然支付成功，则可能导致购买到了一个负数数量的产品，也有可能返还相应的积分/金币到你 的账户上。但是，这种情况不可能发生在通过支付宝支付的订单中(虽然我曾经也想过，但是是不行滴....)，因为显然支付宝是不支持一个负数金额的订单， 所以这种情况多数发生在一个有站内货币的网站。

- 请求重放漏洞

未采用动态加密方法的认证过程，可能导致业务系统的认证功能失效。

例如对重要的操作，如转账操作，先正常进行一个正常的流程，在流程的重要环节，对提交的数据进行同时拦截，对取得的数据再次进行提交，如提交返回结果成功，则此流程存在重放攻击漏洞，反之则满足设计安全要求

- 欺骗密码找回漏洞

目前业务系统对于用户的口令找回，有多种实现逻辑，其中很可能存在验证漏洞从而导致密码泄露。

5. 移动 APP 安全渗透测试检查类

随着运营商新技术新业务的发展，运营商集团层面对安全的要求有所变化，渗透测试工作将会面临内容安全、计费安全、客户信息安全、业务逻辑及 APP 等方面的挑战。随着运营商自主开发的移动 APP 越来越多，这些 APP 可能并不会通过应用市场审核及发布，其中的安全性将面临越来越多的挑战。

5.1 评估思路

移动 APP 面临的威胁风起云涌的高科技时代，随着智能手机和 iPad 等移动终端设备的普及，人们逐渐习惯了使用应用客户端上网的方式，而智能终端的普及不仅推动了移动互联网的发展，也带来了移动应用的爆炸式增长。在 APP 安全测试实例中，APP 安全评估集中在 7 个方面：敏感信息安全、认证鉴权、能力调用、资源访问、通信安全、键盘输入及反逆向。

5.2 测试方式

5.2.1 静态测试

1）签名检查

2）应用权限

3）文件分析

4）反编译

5）调试开关

6）二次打包

5.2.2 动态测试

1）数据文件

2）调试信息

3）组件通信

4）网络通信

5）键盘测试

6）截屏测试

5.2.3 服务端测试

1）认证

2）密码管理

3）会话管理

4）权限控制

5）注入

6）跨站

5.3 常用工具

1） 平台：JDK、ADT

2） 反编译、打包：Jeb、apktool、dex2jar、jd-gui

3） 代理：Burp suite 、ProxyDroid

4） 组件通迅：Drozer

5） 辅助：Firefox、Hackbar

5.4 Androidmanifest.xml 分析

5.4.1 目的：

1）识别应用滥用的权限

2）检测调试功能是否开启

3）分析支持外部调用的组件

4）文件中 allowBackup 属性值被设置为 true

5）webview 漏洞 addJavascriptInterface

5.4.2 检查方法

1)使用 JDB 反编译

2） 使用 apktool 提取资源

5.5 应用权限测试

5.5.1 目的

1)识别应用滥用的权限

5.5.2 检查方法

1）使用 JDB 反编译

2） 使用 apktool 提取资源

5.6 应用文件分析

5.6.1 目的

1）发现敏感文件，搜集有用的信息

2）重点关注目录

5.6.2 检查方法

重点关注文件：

（1）配置类文件，如：XML\PROPERTIES\INI 等类型文件

（2）功能性文件：如：html\js\so 等类型文件

（3） 密钥类文件，如：cer\crt\pfx 等类型文件

5.7 数据文件检验

5.7.1 目的

检查是否有敏感信息泄露，代码使用弱加密技术对敏感信息资产进行加密

5.7.2 检查方法

1）启动 APP 并成功登录

2）使用 Android Debug Monitor 连接测试设备

3）检查数据目录下的文件

5.7.3 重点关注目录

1）shared_prefs

2)dbfile

3)files

5.8 调试信息测试

5.8.1 目的

检查 APP 是否输出了敏感的调试信息，包括不安全的数据存储和非故意的数据泄漏。

5.8.2 检查方法

1）使用 android Debub Monitor 连接测试设备

2）启动 APP 登陆后进行各项操作

3）检查 android debug monitor 上 logcat 的输出信息

5.8.3 重点关注

1）URL 及传输

2）帐号、密码

3） 其它敏感信息

5.9 组件通信测试

5.9.1 目的

分析组件攻击面（识别 exported 组件），包括不健全的握手通信过程、SSL 版本的不正确使用、脆弱协议、敏感信息的明文传输等。

对支持导出的 activity、service、contentprovider 进行测试。

5.9.2 参考案例

1)应用使用手持密码锁定时，通过调用 Activity 绕过手势密码

2）调用 service 传入外部下载 URL，使更新功能下载安装任意文件

3）调用 contentprovider 检测 APP 是否存在注入问题

4） 调用 contentprovider 获取或修改应用数据库中的敏感信息

5.10 键盘输入测试

5.10.1 目的

1）检查密码是否可直接被窃取

5.10.2 检查方法

1）检查密码输入使用的键盘类型

2）观察键盘的布局变化

3）检查用户输入的屏幕响应

4）键盘记录测试，替换系统软键盘，检查输入是否会被记录

5）软键盘随机布局测试：多次进入密码输入状态，观察键盘布局变化

5） 截屏测试：当用户输入过程中连续截取屏幕

5.11 越权测试

5.11.1 目的

发现用户间越权行为、发现未授权访问行为，包括对终端用户身份验证或坏的会话管理的意见。这可以包括：当被要求时，没有对所有用户进行身份识别。当被要求时，没有保持对用户身份的确认。会话管理中的漏洞。

5.11.2 检查方法

1）需要至少 2 个用户 A 和 B

2）收集所有只应用户有权限的请求

3）注销 A 用户，登陆 B 用户，提交手机的请求，分析结果

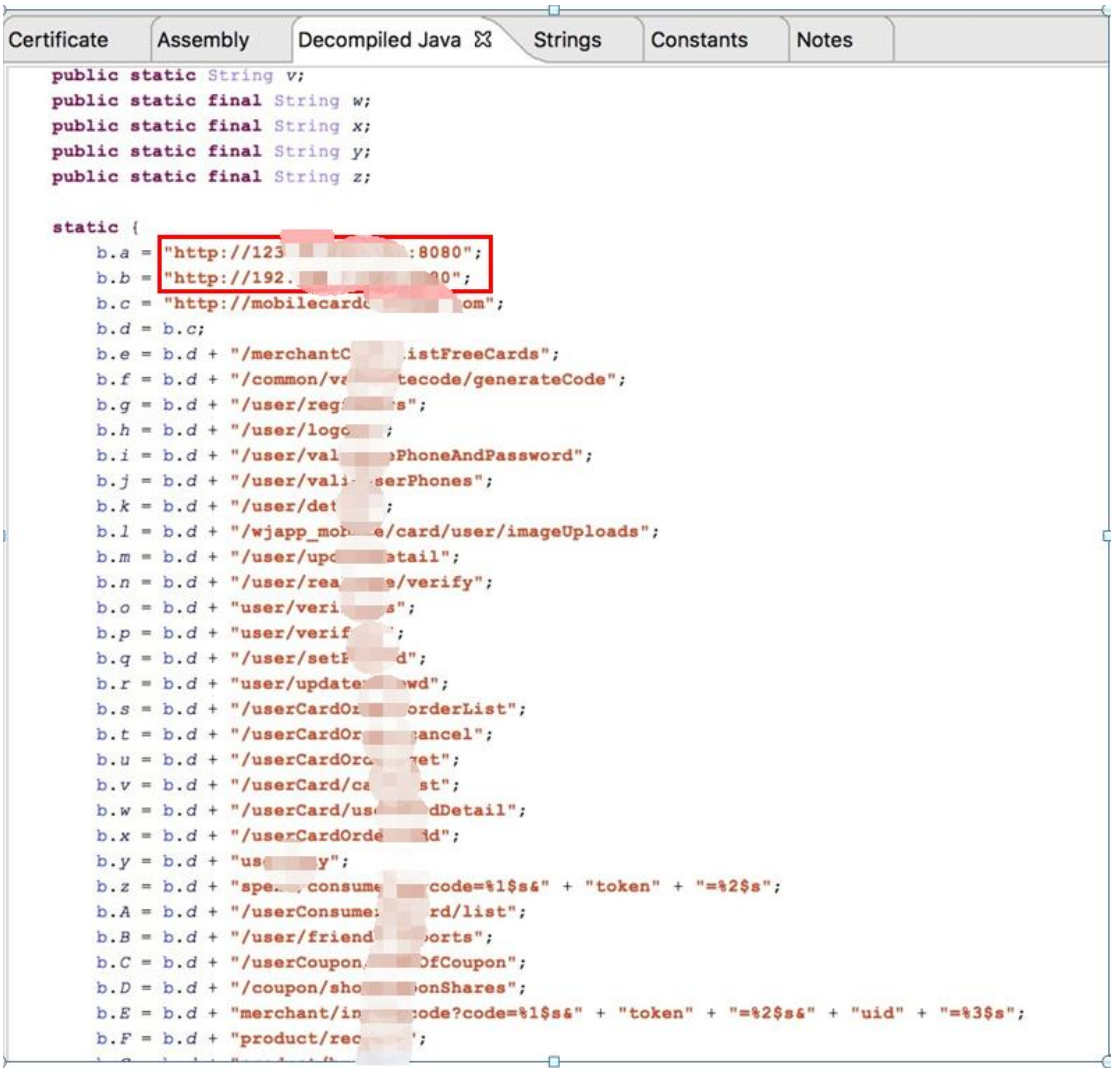
4）未登陆时提交请求，分析请求结果

5.11.3 测试方法

1） 条件允许的情况下建议用 Firefox+hackbar+modifyheaders 模拟客户端

5.12 APP 渗透案例展示

5.12.1 通过逆向 APP 找到测试地址：



可以通过调试模式备份数据

AllowBackup=True

5.12.2 通过逆向 APP 编写解密程序

APP 数据包可逆向，按照加密程序编写解密脚本。

```php
<?php
$data=$argv[1];
$data=  urldecode($data);
$datas=  split("\=", $data);
print_r($datas);
$data0=$datas[0];
$data1=$datas[1];
$data2=$datas[2];

echo '数据1: '. (base64_decode(strrev($data0))."\r\n";
$data1=  substr($data1, 0,5).substr($data1, 6);
echo '数据2: '.  base64_decode($data1)."\r\n";
echo '数据3: '.base64_decode($data2)."\r\n";
```

```
Array
(
    [0] => w4SMu0iLu0iLwkjNzMzNxIjMzEjLt4iN1QzM
yEjLt4CNuQjL04SLuMkMlMkMlUjRBNTJBRUQzUSMEF0MlgTOBNTJ0QTQzUCO1MkMlUDN5M2M2IDZ
zImM4EjZmF2QyUSM2AjM3ITMyAzMzQDO2gzQyUSZ1JHdu0iLBJDMyUSTI5SLuAjL04iMu0iLy8lM
    [1] => MDAwLw3VzZXIvdmFsaWRhdGVQaG9uZUFuZFBhc3N3b3Jk
    [2] => ODZiMmNhNWVlYThlZGJlZjIwNzU5YTBhYjQwYmFjYjYwOTI2ZTJlMg
    [3] =>
    [4] =>
)
数据1: 2_2.-.2.4.0.-.HM&202A.-.true%2C86843302127206l%2Caff182b3d263c945%2C58%3A44%3A98%3AD1%3ADA%3AF5%2C%
2C.-.4.4.4.-.123456.-.13221733690.-..-.1.0
数据2: 000/user/validatePhoneAndPassword
数据3: 86b2ca5eea8edbef20759a0ab40bacb60926e2e2
```

设置新密码,密码未做 hash 传输

解密后的数据密码明文传输：

```
数据1: 2_2.-.2.4.0.-.HM&202A.-.true%2C[redacted]%2Caff182b3d263c945%2C58%3A44%3A98%3AD1%3ADA%3AF5%2C%2C.-.4.4.4.-.123456.-.9cb59aa4967c9b6f4
a0bba6b3ff2b03a.-.1.0
数据2: 000/user/setPaypwd
数据3: de65a197f9bac8caf14b9ce4dfc6c3e4f1c8269e
2_2.-.2.4.0.-.HM 2A.-.true,[redacted],aff182b3d263c945,58:44:98:D1:DA:F5,,.-.4.4.4.-.123456.-.9cb59aa4967c9b6f4a0bba6b3ff2b03a.-.
```

传输中的加密数据

sid=w4SMu0iLhNDMiJjZmNjY2EmYiBTY0YmNilzY3YTO0EWY5UjYjljLt4iN1QzM%0AyE
jLt4CNuQjL04SLuMkMlMkMlUjRBNTJBRUQzUSMEF0MlgTOBNTJ0QTQzUCO1MkMlUDN5M2
M2IDZ%0AzImM4EjZmF2QyUSM2AjM3ITMyAzMzQDO2gzQyUSZ1JHdu0iLBJDMyUSTI5SLu
AjL04iMu0iLy8lM%3DMDAwLw3VzZXIvc2V0UGF5cHdk%3DZGU2NWExOTdmOWJhYzhjYWY
xNGI5Y2U0ZGZjNmMzZTRmMWM4MjY5ZQ%3D%3D

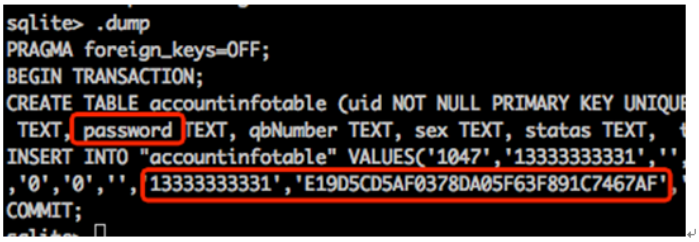
5.12.3 本地数据库数据明文存储

- 2.7. 本地机要数据明文存储

漏洞地址: IOS 客户端应用目录 Documents/[redacted]Database/[redacted]ata.db

危险等级: 中

漏洞说明: sqlite 数据库中明文存储用户信息.



漏洞危害: 在越狱设备运行该应用,可导致用户账号和加密密码信息被其他应用程序读取,导致用户账号信息泄露.

- 2.3. 短信验证码在回包中返回(可强制注册/重置任意用户密码)

漏洞地址: http://im[redacted]com/overseas/user/valicode

POST 数据: account=账号&telCode=86&type=1

危险等级: 高

漏洞说明: 在发送验证码的响应中,包含了系统发送给手机的验证码,且在下一步的验证中,App 采用了本地验证,该验证步骤实际可被绕过.

漏洞危害: 通过该漏洞,可强制任意手机号码注册,或重置任意用户密码.

2.4. 系统无会话控制机制

漏洞地址: 系统登录后,无会话管理机制.直接通过相关接口,通过用户 uid 进行信息获取操作.

危险等级:中

漏洞说明: 经过分析登录后的业务请求数据,发现系统无有效的会话控制机

制.

漏洞危害: 由于无会话管理机制,因此此处可查询任意用户的包括但不限于用户的个人信息,用户的好友信息等(可参考之后的多个漏洞)

6. APT 检测

7.1 APT 概述

APT（Advanced Persistent Threat）--------高级持续性威胁。 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，APT 攻击的原理相对于其他攻击形式更为高级和先进，其高级性主要体现在 APT 在发动攻击之前需要对攻击对象的业务流程和目标系统进行精确的收集。在此收集的过程中，此攻击会主动挖掘被攻击对象受信系统和应用程序的漏洞，利用这些漏洞组建攻击者所需的网络，并利用 0day 漏洞进行攻击。

7.2 APT 测试流程

对重点目标进行 APT 测试，分为以下几个流程：

7.2.1 信息收集

专业安全工具扫描：专业安全工具扫描、嗅探，对系统的网络、主机和应用程序进行远程漏洞扫描，并对扫描结果进行分析。

社会工程学探查：利用社会工程学结合大数据方式获取目标网站信息，例如：邮箱、QQ，手机号，身份证信息，历史密码等信息。

7.2.2 单点攻击

收集了足够的信息后，采用恶意代码攻击组织员工的个人电脑，获取后台或个人终端操作权限。

7.2.3 控制通道构建

通过获得操作权限的后台或个人终端，构建某种渠道和测试人员取得联系，以便进一步发送攻击指令。

7.2.4 内部横向渗透

以被攻击个人电脑或后台为跳板，在系统内部进行横向渗透，以攻陷更多的 PC 和服务器。测试人员采取的横向渗透方法包括口令窃听和漏洞攻击等。

7.2.5 数据收集上传

将重要数据资产，进行压缩、加密和打包，然后通过隐蔽的数据通道将数据传回。

7.2.6 报告编写

APT 测试报告包括 APT 测试整个流程描述，会对发现问题的思路与手法进行必要的说明，并且结合目标系统环境，对安全问题进行风险分析，出具针对性解决方案。

7. 漏洞扫描服务

7.1. 漏洞扫描服务简介

漏洞扫描服务为迎合客户对于解决高风险漏洞和当前网络漏洞分布情况的了解需求而退出。是根据知道创宇多年安全行业从业经验，基于自主开发的漏洞扫描设备 Websoc 的安全服务。

7.2. 漏洞扫描服务方式分类

7.2.1.内部扫描与外部扫描

内部扫描是指，安全服务人员在用户现场直接介入到用户内部网络，对目标系统安全扫描的行为。内部测试主要针对以下情况：

- 需绕过边界防护设备

  被测试的目标系统置于边界防护设备之后，且边界防护设备的有效性和安全性不包含在测试要求中的情况下，可通过接入到网络内部来实现对目标系统的直接、无防护的访问。

相对内部测试而已，外部测试则是指扫描人员直接从互联网对目标系统进行安全扫描。

7.3. 漏洞扫描服务内容

7.3.1.专业、完善的漏洞扫描报告

通过知道创宇自主研发的 websoc 专业漏洞扫描工具，为客户提供专业的漏洞扫描报告，包括详细的漏洞风险说明、影响的系统类型和版本、安全解决建议等，及时发现风险，及时修补加固；

7.3.2.闭环处理漏洞生命周期

帮助客户实现闭环处理漏洞管理，从资产发现，漏洞扫描，漏洞检查报告，漏洞修补，修补效果验证；

7.3.3.定期监测，实时更新

完全贴合客户需求，针对目标系统的扫描周期可以随时调整，并保证扫描设备的特征库随时处于最新版本状态；

7.4. 漏洞扫描服务优势

- 无需购买专业软件、硬件漏洞扫描产品，漏洞扫描服务所需的人员、设备均由厂商提供；实时生效；
- 无需专业人员维护，可定期自动持续监控，并生成报告；
- 人工验证漏洞报告，保证输出报告有效性；
- 按需购买，最大化利用资金；

8. 渗透测试输出报告

渗透测试完成后的两个工作日内，渗透测试人员将输出最终版渗透测试报告。渗透测试报告包含渗透测试的整个流程描述，同时，还会对发现安全问题的思路与技术手法进行必要的说明，并结合测试目标所处的业务环境，对安全问题进行风险分析（如：可能产生的后果等方面）。除此以外，测试人员还将针对发现的问题提出具有针对性的解决方案，以便用户在修复过程中参考。

9. 各类型渗透服务差异对比

9.1. 高级渗透测试、专业渗透测试与漏洞扫描服务差异对比

在 Web 安全测试服务方面，知道创宇安全服务部有高级渗透测试服务、专业渗透测试及安全漏洞扫描三种服务。

- 高级渗透测试针对业务重要性高，页面功能复杂的客户，针对各个类型的 web 应用提供安全渗透测试服务，服务周期长、检测深度足够，对业务逻辑漏洞尤为关注；
- 专业渗透测试服务作为知道创宇推出的一款中级 Web 安全服务，在检测

内容方面与高级渗透测试服务存在差异，但是服务周期适中；

- 安全漏洞扫描服务是一款轻量级 Web 安全服务，针对 Web 业务简单，但有周期性检查需求的客户，服务周期短，检测范围广，对 Web 漏洞采用人工验证，以确保报告中漏洞信息的准确性。

三款服务产品对比如下；

阶段	工作明细	高级渗透测试	专业渗透测试	安全漏洞扫描
信息收集	网站工具扫描	√	√	√
	信息收集	√	√	√
	客户前端交流	√	√	×
	社会工程学探查	√	√	×
保密承诺	客户信息保密	√	√	√
扫描初步分析	OWASP TOP10	√	√	√
	WASC Web威胁	√	√	√
	漏洞扫描报告分析	√	√	√
	服务器信息分析	√	√	√
	业务动态感知	√	×	×
人工验证	漏洞分析	√	√	√
	漏洞交互分析	√	√	×
	账号、路径分析	√	×	×
	业务逻辑、功能分析	√	×	×
提权	获取后台账号权限	√	√	×
漏洞深度挖掘	资产风险分析	√	×	×
	授权绕过漏洞分析	√	×	×
	截获和修改金额漏洞分析	√	×	×
	规避交易限制分析	√	×	×
	请求重放漏洞测试	√	×	×
	欺骗密码找回漏洞测试	√	×	×
	顺序执行缺陷漏洞分析	√	×	×
	后台资料下载	√	×	×
	网站挂马查杀	√	×	×
报告生成&解答	报告制作	√	√	√
	人工答疑	√	√	√
交付周期		2周左右	1周内	3工作日内

9.2. 渗透测试与众测服务差异对比

知道创宇的渗透测试服务不用于目前新起于“互联网+”概念的“众测”，由于众测服务模式的特殊性，导致了客户资产安全的不确定性，而在众多检测内容与交付质量上，“众测”也是难以提供可靠的保障的。部分差异如下表：

服务名称 / 对比项	高级渗透测试	专业渗透测试	安全众测
业务、功能对比			
项目周期（/域名）	15 工作日	3 工作日	10 至 15 工作日
售价（/域名）	￥50000 左右	￥9998	￥30000 左右
传统域名测试	√	√	√
APP 安全测试	√	√	√
漏洞信息公开隐患	无	无	可能
技术团队可靠性	技术人员稳定、可靠	技术人员稳定、可靠	人员能力随机
报告制作、人工讲解	√	√	无人工讲解
最新漏洞通告（可选）	×	√	×
网站性能监控（可选）	×	√	×
实施内容对比			
目标信息收集	√	√	√
系统漏洞识别	√	√	√
注入漏洞识别	√	√	√
XSS 与 CSRF 利用	深入关联利用	仅识别、指出漏洞	√
重定向检测	深入关联利用	仅识别、指出漏洞	√
业务逻辑错误	√	×	√
口令认证错误	√	部分验证	√
渗透结果关联测试	√	×	√

10. 应急响应

10.1. 传统计算机病毒攻击

10.1.1. 概念

传统计算机病毒特指不能通过电子邮件、网站页面等常见互联网服务进行直接传播和感染的计算机病毒。

10.1.2. 攻击特征描述

病毒必须满足两个条件: 1、它必须能自行执行。它通常将自己的代码置于另一个程序的执行路径中。 2、它必须能自我复制。例如，它可能用受病毒感染的文件副本替换其他可执行文件。病毒既可以感染桌面计算机也可以感染网络服务器。 此外，病毒往往还具有很强的感染性，一定的潜伏性，特定的触发性和很大的破坏性等。

一些病毒被设计为通过损坏程序、删除文件或重新格式化硬盘来损坏计算机。有些病毒不损坏计算机，而只是复制自身，并通过显示文本、视频和音频消息表明它们的存在。即使是这些良性病毒也会给计算机用户带来问题。通常它们会占据合法程序使用的计算机内存。结果，会引起操作异常，甚至导致系统崩溃。另外，许多病毒包含大量错误，这些错误可能导致系统崩溃和数据丢失。

10.1.3. 应急处理办法

如果在网络中发现此类病毒，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此病毒的详细说明、造成的影响以及病毒类型；通过事件的详细描述进行病毒源的有效定位，查到源 IP、目的 IP，对感染终端进行断网隔离，然后通过杀毒软件、人工查杀等方式进行处理。

10.1.4. 安全建议

1) 网络中安装防火墙，每当有不明的程序想要进入系统，或者连出网络，防火墙都会在第一时间拦截，并检查身份，如果是经过许可放行的

2) 及时更新系统漏洞补丁；

3) 对公用软件和共享软件要谨慎使用，使用 U 盘时要先杀毒，以防 U 盘携带病毒传染计算机。

4) 从网上下载任何文件后，一定要先扫描杀毒再运行。

5) 对重要的文件要做备份，以免遭到病毒侵害时不能立即恢复，造成不必要的损失。

6) 对已经感染病毒的计算机，可以下载最新的防病毒软件进行清除。

10.2. 邮件病毒攻击

10.2.1. 概念

邮件病毒是指通过电子邮件方式进行传播和感染的计算机病毒。

10.2.2. 攻击特征描述

电子邮件攻击就是对某个或多个邮箱发送大量的邮件，从而充满邮箱，大量的占用了系统的可用空间和资源。使网络流量加大占用处理器时间，消耗系统资源，从而使系统瘫痪，无法正常工作。大量的垃圾信件还会占用大量的 CPU 时间和网络带宽，造成正常用户的访问速极慢，导致邮件服务器崩溃，甚至造成整个网络中断。

10.2.3. 应急处理办法

如果在网络中发现此类病毒，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此病毒的详细说明、造成的影响以及病毒类型；通过事件的详细描述进行病毒源的有效定位，查到源 IP、目的 IP，对感染终端进行断网隔离，然后通过杀毒软件、人工查杀等方式进行处理。

10.2.4. 安全建议

1) 安装杀毒软件；对于邮件附件尽可能小心。因为有的病毒邮件恶毒之极，只要你将鼠标移至邮件上，哪怕并不打开附件，它也会自动执行。

2) 设置文件夹选项，显示文件名的扩展名。这样一些有害文件，如 VBS 文件就会原形毕露。

3) 千万别打开扩展名为 VBS、SHS 和 PIF 的邮件附件。这些扩展名从未在正常附件中使用，但它们经常被病毒使用。对于有 2 个扩展名的附件，比如*.BMP.EXE 或者*.TXT.VBS 文件，亦要万分小心。

4) 一般情况下勿将磁盘上的目录设为共享，如果确有必要，请将权限设置为只读，读操作须指定口令。

5) 如果你觉得从朋友那里来的邮件有点奇怪，暂不要打开，待向朋友确认之后再处理不迟。

6) 当你收到邮件广告或者主动提供的电子邮件时，不要打开附件以及它提供的链接。

7) 将游览器的隐私设置设为“高”。

10.3. 蠕虫攻击

10.3.1. 概念

蠕虫病毒特指除邮件病毒以外，利用网络与信息系统缺陷，通过网络自动传播的计算机病毒。

10.3.2. 攻击特征描述

蠕虫病毒作为对互联网危害严重的一种计算机程序，其破坏力和传染性不容忽视。与传统的病毒不同，蠕虫病毒以计算机为载体，以网络为攻击对象。复制自身在互联网环境下进行传播，蠕虫会开启多个线程大面积传播，在传播过程中占用宽带资源，从而达到攻击的目的，，病毒的传染能力主要是针对计算机内的文件系统而言;而蠕虫病毒的传染目标是互联网内的所有计算机.局域网条件下的共享文件夹，电子邮件，网络中的恶意网页，大量存在着漏洞的服务器等都成为蠕虫传播的良好途径。

10.3.3. 应急处理办法

如果在网络中发现此类病毒，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此病毒的详细说明、造成的影响以及病毒类型；通过事件的详细描述进行病毒源的有效定位，查到源 IP、目的 IP，对感染终端进行断网隔离，然后通过杀毒软件、人工查杀等方式进行处理。

10.3.4. 安全建议

1) 提高自己的安全意识，不要轻易去点击陌生的站点。

2) 使用具有实时监控功能的杀毒软件，经常升级病毒库。

3) 不随意查看陌生邮件，尤其是带有附件的邮件。

10.4. 脚本攻击

10.4.1. 概念

脚本病毒是指通过 JavaScript、VBScript、ActiveX 等网页脚本语言方式进行传播和感染的计算机病毒。

10.4.2. 攻击特征描述

脚本攻击就是利用这些文件的设置和编写时的错误或者疏忽不当来达到传播和感染计算机病毒的攻击目的。

10.4.3. 应急处理办法

如果在网络中发现此类脚本攻击，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此脚本攻击的详细说明、造成的影响以及病毒类型；通过事件的详细描述进行脚本攻击源的有效定位，查到源 IP、目的 IP，对感染终端进行断网隔离，然后通过杀毒软件、人工查杀等方式进行处理。

10.5. 木马程序攻击

10.5.1. 概念

木马程序是指潜伏在电脑中，受外部用户控制以窃取本机信息或者控制权的程序。木马程序危害在于多数有恶意企图，例如占用系统资源，降低电脑效能，危害本机信息安全，将本机作为工具来攻击其他设备等。

这里所说的木马程序攻击是由于制造、传播或因受到木马程序影响而导致的信息安全事件。

10.5.2. 攻击特征描述

- **隐蔽性**

木马必需隐藏在系统之中，它虽然在系统启动时会自动运行，但它不会在“任务栏”中产生一个图标；木马程序自动在任务管理器中隐藏，并以“系统服务”的方式欺骗操作系统。

- **自动运行性**

它是一个当你系统启动时即自动运行的程序，所以它必需潜入在你的启动配置文件中，如 win.ini、system.ini、winstart.bat 以及启动组等文件之中。

- **欺骗性**

木马程序要达到其长期隐蔽的目的，就必需借助系统中已有的文件，以防被你发现，它经常使用的是常见的文件名或扩展名

- **自动恢复功能**

现在很多的木马程序中的功能模块已不再是由单一的文件组成，而是具有多重备份，可以相互恢复。

- **自动打开端口**

木马程序潜入电脑之中的目的是为了获取系统中有用的信息，这样就必需在上网时能与远端客户进行通讯，这样木马程序就会用服务器/客户端的通讯手段把信息告诉黑客们，以便黑客们控制你的机器，或实施更加进一步入侵企图。

- **特殊性**

通常的木马的功能都是十分特殊的，除了普通的文件操作以外，还有些木马具有搜索 cache 中的口令、设置口令、扫描目标机器人的 IP 地址、进行键盘记录、远程注册表的操作、以及锁定鼠标等功能。

10.5.3. 应急处理办法

如果在网络中发现此类木马病毒，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此木马病毒的详细说明、造成的影响以及木马病毒类型；通过事件的详细描述进行木马病毒源的有效定位，查到源 IP、目的 IP，对感染终端进行断网隔离，然后通过杀毒软件、人工查杀等方式进行处理。

简单的说，主要的应急处理办法有 2 条：

① 木马查杀

② 删除木马病毒

10.5.4. 安全建议

1) 关闭不必要的Ｗｉｎｄｏｗｓ服务。

2) 对于其他木马或蠕虫病毒默 认端口或不安全端口， 可以使用专用的安全工具或对注册表 进行操作等方法进行关闭。

3) 停用来宾账户，同时清除不必 要的账户。

4) 设定坚固的安全密码。

5) 正确设置账户锁定策略， 防止入侵者不断尝试破解登录密码的企图。

6) 文件共享策略谨慎设置，确实有需要时才开放文件共享。用完立即关闭。

10.6. 其他恶意代码攻击

10.6.1. 概念

恶意代码是指独立的程序或者嵌入到其他程序中的代码，它在不被用户察觉的情况下启动，利用其他方式对网络与信息系统实施攻击的网络与信息安全事件，达到破坏电脑安全性和完整性的目的。

10.6.2. 攻击特征描述

恶意代码具有如下共同特征：（1） 恶意的目的（2） 本身是程序（3） 通过执行发生作用。

10.6.3. 应急处理办法

如果在网络中发现此类恶意代码攻击，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此攻击的详细说明、造成的影响以及攻击类型；通过事件的详细描述进行攻击源的有效定位，查到源 IP、目的 IP，对感染终端进行断网隔离，然后通过杀毒软件、人工查杀等方式进行处理。

10.6.4. 安全建议

1) 不要轻易去一些并不十分知晓的站点，否则往往不经易间就会误入网页代码的圈套。

2) 当运行 IE 时，点击“工具→Internet 选项→安全→ Internet 区域的安全级别”，把安全级别由“中”改为“高” 。

3) 在 IE 设置中将 ActiveX 插件和控件、Java 脚本等全部禁止就可以大大减少被网页恶意代码感染的几率。具体方案是：在 IE 窗口中点击“工具”→“Internet 选项”，在弹出的对话框中选择“安全”标签，再点击“自定义级别”按钮，就会弹出“安全设置”对话框，把其中所有 ActiveX 插件和控件以及与 Java 相关全部选项选择“禁用”。

4) 在终端计算机上安装网络防火墙，并要时刻打开“实时监控功能”。

10.7. 试探性攻击

10.8. 探测性扫描

10.8.1. 概念

探测性扫描攻击指利用网络扫描方式获取信息系统网络配置、端口、服务、存在的脆弱性等特征对网络与信息系统实施攻击而导致的信息安全事件。

10.8.2. 攻击特征描述

入侵者通常会用扫描器对目标主机的端口进行扫描，以确定哪些端口是开放的。从开放的端口，入侵者可以知道目标主机大致提供了哪些服务，进而猜测可能存在的漏洞。当服务器存在漏洞时可能被入侵者探测到，并且进一步通过漏洞入侵服务器。此事件的产生是多数是由于目的 IP 提供某些服务，如 web，其他终端在对此设备进行访问的时候会先测试这台主机是否存活，从而产生该类型的报警。

10.8.3. 应急处理办法

如果在网络中发现此类攻击，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此探测性扫描的详

细说明、造成的影响以及扫描类型；通过事件的详细描述进行扫描主机源的有效定位，查到源 IP、目的 IP，对报警事件进行精确定位。并根据解决建议进行排查和处理。

10.9. 口令试探攻击

10.9.1. 概念

目前口令试探攻击主要是通过密码破解程序来实现。口令破解程序大多采用字典攻击以及暴力攻击手段，通过字典攻击或者是社会工程的手段来破解口令，从而引发对网络与信息系统实施攻击的网络与信息安全事件。

10.9.2. 应急处理办法

如果在网络中发现此类攻击，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此探测性扫描的详细说明、造成的影响以及扫描类型；通过事件的详细描述进行扫描主机源的有效定位，查到源 IP、目的 IP，对报警事件进行精确定位。并根据解决建议进行排查和处理。

10.9.3. 安全建议

1) 建议用户在设定密码的过程中尽量使用非字典中出现的组合字符，并且采用数字与字符相结合、大小写相结合的密码设置方式，增加密码被黑客破解的难度。

2) 不要只使用单词或数字，决不要在口令中只使用单词或数字。

3) 千万不要使用个人信息。

4) 不要笔录自己的口令。

5) 要在所有机器上都使用同样的口令：

6) 使用定期修改密码、使密码定期作废的方式来保护登录密码的安全。

10.10. 网络监听攻击

10.10.1. 概念

在网络进行信息传播的时候，可以利用工具将网络接口设置在监听的模式，

便可将网络中正在传播的信息截获或者捕获到，从而进行攻击。

10.10.2. 攻击特征描述

网络监听一般很难被发现。当运行监听程序的主机在监听的过程中只是被动的接收在以太网中传输的信息，它不会跟其它的主机交换信息的，也不能修改在网络中传输的信息包。

网络监听在网络中的任何一个位置模式下都可实施进行。而黑客一般都是利用网络监听来截取用户口令。在占领了一台主机之后，通过网络监听的方式截取到用户口令后，通过此台被监听的主机进行将攻击范围扩大到这个主机所在的整个局域网。

网络监听没有主动行为的发生，但运行网络监听的主机需不断地响应从网卡传来的数据包。所以，会消耗大量的资源。因此，监听软件机器的运行特征是：系统会因负荷过重，对外界的响应很慢。

10.10.3. 应急处理办法

针对此类监听攻击，建议通过人工方式进行系统反应时间的检测。向有网络监听行为的网络发送大量的测试数据包，再依各主机回应情况判断，正常的系统回应的时间无明显变化，而处监听模式的系统对大量的测试信息照单全收，所以回应时间有较大变化。

同时，许多网络监听软件会尝试对地址反向解析。可观测被怀疑主机的 DNS 系统是否明显增多的解析。

如通过上述应急排查发现有此类攻击存在，建议对网络中的数据，尤其是明文的秘密数据，采用加密算法进行加密是很好的解决办法。 此外，用户可使用拓扑结构（称为分段技术）， 将网络分成小的子网。依网络结构使用路由器来分段，网段间是硬件连接，黑客很难攻入。

10.11.网络与系统攻击

10.12.拒绝服务攻击

10.12.1. 概念

拒绝服务攻击事件是指利用信息系统缺陷、或通过暴力攻击的手段，以大量消耗信息系统的 CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系

统正常运行为目的的信息安全事件。

10.12.2. 攻击特征描述

攻击者进行拒绝服务攻击，实际上会实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。

异常现象 1：当 DDoS 攻击一个站点时，会出现明显超出该网络正常工作时的极限通讯流量的现象。

异常现象 2：特大型的 ICP 和 UDP 数据包。

异常现象 3：不属于正常连接通讯的 TCP 和 UDP 数据包。

异常现象 4：数据段内容只包含文字和数字字符的数据包。

异常现象 5：数据段内容只包含二进制和 high-bit 字符的数据包。

10.12.3. 应急处理办法

如果在网络中发现此类攻击，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此病毒的详细说明、造成的影响以及病毒类型；通过事件的详细描述进行病毒源的有效定位，查到源 IP、目的 IP，对感染终端进行断网隔离，然后通过杀毒软件、人工查杀等方式进行处理。

同时，还可以通过管理人员的人工方式对一些设置做一些限制，如限制可以使用的最大内存、CPU 时间以及可以生成的最大文件等，也能很好的规避此类安全风险的出现。

10.13.后门攻击

10.13.1. 概念

后门攻击是指利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施的攻击的信息安全事件；

10.13.2. 攻击特征描述

后门攻击可以非法地取得用户电脑的超级用户级权利，可以对其进行完全的控制，除了可以进行文件操作外，同时也可以进行对方桌面抓图、取得密码

等操作。这些后门软件分为服务器端和用户端，当黑客进行攻击时，会使用用户端程序登陆上已安装好服务器端程序的电脑，这些服务器端程序都比较小，一般会随附带于某些软件上。

后门产生的必要条件有以下三点：

- 必须以某种方式与其他终端节点相连。
- 目标机默认开放的可供外界访问的端口必须在一个以上。
- 目标机存在程序设计或人为疏忽，导致攻击者能以权限较高的身份执行程序。

10.13.3. 应急处理办法

如果在网络中发现此类攻击，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此攻击的详细说明、造成的影响以及攻击类型；通过事件的详细描述进行攻击源的有效定位，然后根据解决建议进行人工查杀等方式进行处理。

同时，将终端机和服务器上不必要的服务关闭，选定适合的网络接口避免外连的可能；对于公开对外的服务，一定需要及时打上相应的补丁。

10.14.漏洞利用攻击

10.14.1. 概念

漏洞攻击事件（VAI）是指除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件。

10.14.2. 应急处理办法

如果在网络中发现此类攻击，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此病毒的详细说明、造成的影响以及病毒类型；通过事件的详细描述进行病毒源的有效定位，查到源 IP、目的 IP，对感染终端进行断网隔离，然后通过杀毒软件、人工查杀等方式进行处理。

10.14.3. 安全建议

1) 定期对磁盘进行碎片整理和磁盘文件扫描。
2) 维护系统注册表。
3) 经常性地备份系统注册表。
4) 清理 system 路径下的无用的 dll 文件。
5) 使用防系统死机工具维护系统稳定。
6) 使用在线病毒检测工具防止病毒入侵。
7) 使用 windows 辅助工具优化系统。
8) 优化 windows 本身

10.15.其他网络与系统攻击

10.15.1. 概念

其他网络攻击事件（ONAI）是指不能被包含在以上子类之中的网络攻击事件。利用其他方式对网络与信息系统实施攻击的网络与信息安全事件。

10.15.2. 应急处理办法

如果在网络中发现以上此类攻击，首先通过 IDS 设备查看上报过来的 IDS 安全事件，然后在事件库或显示中心里找到对应报警事件，双击该事件，根据 IDS 事件中的“帮助”了解该事件的具体描述，在第一时间了解此攻击的详细说明、造成的影响以及攻击类型；通过事件的详细描和解决建议进行人工查杀等方式进行处理。

11. 专业渗透测试套餐内容

11.1. 专业渗透测试简介

专业渗透测试是通过一系列专业安全服务、工具通过对目标的检测及问题验证发现系统暴露在网络上的脆弱环节。完整的专业渗透测试服务包含：专业渗透测试、漏洞速递服务及网站监控服务。

渗透测试够直观的让管理人员知道自己网络所面临的问题。同时专业渗透测试服务还提供基于微信企业号的漏洞速递，如：漏洞信息、加固方案、安全新闻的每日推送，另外网站性能监控服务也可以让客户在服务周期内对自己的在线应用有更直观的了解及监控手段。

通过：https://www.yunaq.com/security_service/，也可直接查询到相关服务及报价。

11.2. 专业渗透测试概述

与传统操作系统的安全评估不同，针对 WEB 应用的渗透测试没有一个可依赖的、完整的漏洞库可用于检测，因此，在测试过程中，知道创宇会以攻击方式为测试视角，对目标系统进行已知攻击方式的检测，对于已知攻击方式，主要参考 OWASP 组织统计的 63 种常见 WEB 攻击手段，以及 WASC 的 WEB 安全威胁中 34 种 WEB 威胁。

11.3. 专业渗透测试检查项目

11.3.1. 目标信息收集类

11.3.1.1. 目标系统信息探测

目标系统信息探测主要通过端口扫描、banner 信息及指纹监测等方式进行的针对特定服务及端口的版本信息探测过程，通过这些版本信息测试人员可对目标系统进行更具有针对性的测试。

11.3.1.2. 漏洞自动化识别

漏洞自动化识别主要是借助自动化扫描系统从系统层和应用层两个层面，对目标系统发起的漏洞检测工作，系统层面的漏洞检测主要从以下几个方面进行：

- 溢出漏洞
- 口令破解
- 信息泄露

应用层的漏洞检测主要包含以下几个方面：

- 信息泄露
- 配置错误
- 认证破解
- 注入攻击
- 跨站脚本（XSS，Cross Site Script）
- 跨站请求伪造（Cross Site Request Forgery）
- 错误的重定向
- ……

11.3.2. Web 漏洞人工验证类

人工验证的过程主要有几个作用：

1) 对自动化检测结果的校验与验证
2) 利用验证人员的经验深度挖掘漏洞
3) 利用人自身的逻辑识别能力挖掘某些逻辑错误而导致的漏洞

手工漏洞的检测与挖掘，会围绕以下几类漏洞开展。

11.3.2.1. 信息泄露检查

常规自动化检测的信息泄露主要针对某些已知类型的威胁进行的，如：返回页面中包含路径信息、某目录存在匿名目录浏览、某文件存在自动备份文件等等。

但某些信息泄露漏洞往往需要人工介入判断，如，返回信息中存在与目标系统业务具有极大相关性的数据，这些数据的泄露十分危险，但却无法被机械化扫描工具所识别，所以需要人工对此类信息泄露进行挖掘和验证。

11.3.2.2. 注入漏洞验证

注入漏洞分为多种注入方式，如：SQL 注入、XPath 注入、LDAP 注入等等。

不同类型的注入漏洞在利用方式和原理上是相似的，但后台存储的数据内容和用户权限决定了注入漏洞所能获得的收益大小，因此，测试人员手动介入测试注入漏洞时，除验证注入漏洞是否真实存在外，还需对注入漏洞所产生危害的深度与广度进行识别，并结合其影响为该注入漏洞设置合理的危险等级。

11.3.2.3. XSS 与 CSRF 利用

多数 WEB 扫描器对 XSS 与 CSRF 的测试与识别方式单一，一般情况下，扫描器仅仅只能从理论层面验证这类漏洞的存在，但这类漏洞所能带来的安全风险，需由人工辅助来完成鉴别与评估。

11.3.2.4. 重定向检测与利用

重定向漏洞往往被用来与其他漏洞相结合使用，因此，在传统的自动化评估过程中，难以对重定向漏洞进行识别和深度的利用，但通过人工检测的方式，可对重定向漏洞的利用方式及其影响进行重新评估与定义。

11.3.2.5. 参数错误

参数错误分为多种方式，但其中很多设计到逻辑及权限错误的问题时，就难以通过扫描器实现自动识别，对这类错误，往往需要借助渗透工程师的丰富测试经验来进行识别和测试。

11.3.2.6. 逻辑错误

由于逻辑错误并不涉及到程序自身的错误及异常，因此，在自动化检测过程中，逻辑错误是无法被识别的。

逻辑错误不但需要人工进行检测，而且还需要检测人员在检测之前对业务有所了解，因此，在检测前，测试人员往往会构造大量的数据进行测试，以学习业务的正常逻辑，从而进一步构造可能造成业务危害的错误逻辑数据，以达到逻辑测试的目的。

11.3.2.7. 认证错误

认证错误包含多层含义，对于其最简单的理解便是用户登录入口暴露（尤其是敏感用户的登录入口，如：管理登录入口），且存在弱口令或暴力破解的可能（如：无验证码的登录页面即可通过暴力破解的方式尝试通过验证）。

而除此之外，还有某些认证错误是自动化程序无法识别的，例如，登录某系统之后，系统内的任意操作不再对用户身份进行校验，或者，当用户修改口令的时候不对原始口令进行校验，这样的漏洞都可能导致普通用户的越权行为。

11.3.2.8. 漏洞验证

漏洞验证分为三个层面：

- 漏洞是否存在

  某些漏洞是存在的，但其利用成本却较高。

  如：会话破解，会话破解在理论上是可行的，但若目标系统中不存在易猜解的用户口令，则其可利用程度是相当低的，甚至可以说从实际操作上是不可利用的。

  对于此类漏洞，仅具备“存在性”，因此从威胁的定量分析上，其威胁得分也相对较低。

- 漏洞是否可利用

  即，漏洞不但存在，且可利用成功。

- 漏洞利用后获得的权限

  成功后的权限决定了漏洞的危险等级，利用成功后所获得权限越高，恶意用户所产生的恶意行为危害也就越大，其危险等级也就越高。

11.3.3. 渗透测试工作的作用与收益

2） 技术安全性的验证

渗透测试作为独立的安全技术服务，其主要目的就在于验证整个目标系统的技术安全性，通过渗透测试，可在技术层面定性地分析系统的安全性。

3） 查找安全隐患点

渗透测试是对传统安全弱点的串联并形成路径，最终通过路径式的利用而达到模拟入侵的效果。所以，在渗透测试的整个过程中，可有效的验证每个安全隐患点的存在及其影响程度。

4） 安全技能的提升

一份专业的渗透测试报告不但可为用户提供作为案例，更可作为常见安全原理的学习参考。

11.3.4. 渗透测试工作方式说明

11.3.4.1. 自动测试

自动测试是指借助系统和应用扫描工具对站点的系统层和应用层进行全面的安全扫描，以此种方法来检测目标系统中是否包含已知的安全问题。

因自动测试的方式借助了自动化的扫描工具，因此其优点在于检测速度较快，而且对已知漏洞的检测也较为全面。而它的缺点也显而易见：

- 自动化工具对于某些特殊的信息无法实现自动甄别
- 一些复杂的客户端脚本无法完全实现自动检测
- 一些具有较强逻辑性的业务无法通过自动化工具实现检测
- 自动化工具均无法避免误报

11.3.4.2. 黑盒方式

黑盒测试愿意是指，把程序看作一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下，通过测试来检测每个功能是否都能正常使用。

在网站安全体检中，黑盒测试则是指，测试人员在仅获得目标的 IP 地址或域名信息的情况下，对目标系统发起模拟入侵的尝试。

11.3.4.3. 手动测试

手动测试作为自动测试的一种补充，是网站安全体检过程中必不可少的一个重要部分。一般手动测试主要涵盖以下几个方面：

- 对自动测试结果的验证

  自动化检测工具难免存在误报，因此，手动测试过程中需要筛选自动化检测结果中的误报，同时还要对正确告警的结果进行验证和再利用，以确认其危险程度与自动扫描结果一致

- 个性化页面信息的人工甄别

  多数自动化测试工具，其检测条件都是以页面返回页面中的关键字或

HTTP 状态值作为判断条件，而某些经过精心构造的个性化页面，其返回内容可能无法完全由自动化工具进行判断，因此，针对这样的站点就需由人工进行手动测试

由此可见，手动测试会在深度与广度两方面弥补自动化测试的不足，是保障网站安全体检质量的一个重要手段，也是渗透测试的精髓所在。

11.3.5. 渗透测试服务流程

渗透测试的服务流程如下：

渗透测试流程图

11.3.5.1. 安全体检

采用知道创宇 ZoomEye pro、Websoc、CloudEye 和知道创宇专业渗透工具包，对不同类型网站定制扫描、嗅探策略，对系统的主机和应用程序进行远程安全扫描；同时对检测期间目标网站的可用性进行监控。

11.3.5.2. 人工验证

对专业安全工具的扫描结果采用 Metasploit、Burpsuite、Hackbar 等进行人工验证，并且验证安全问题的有效性。

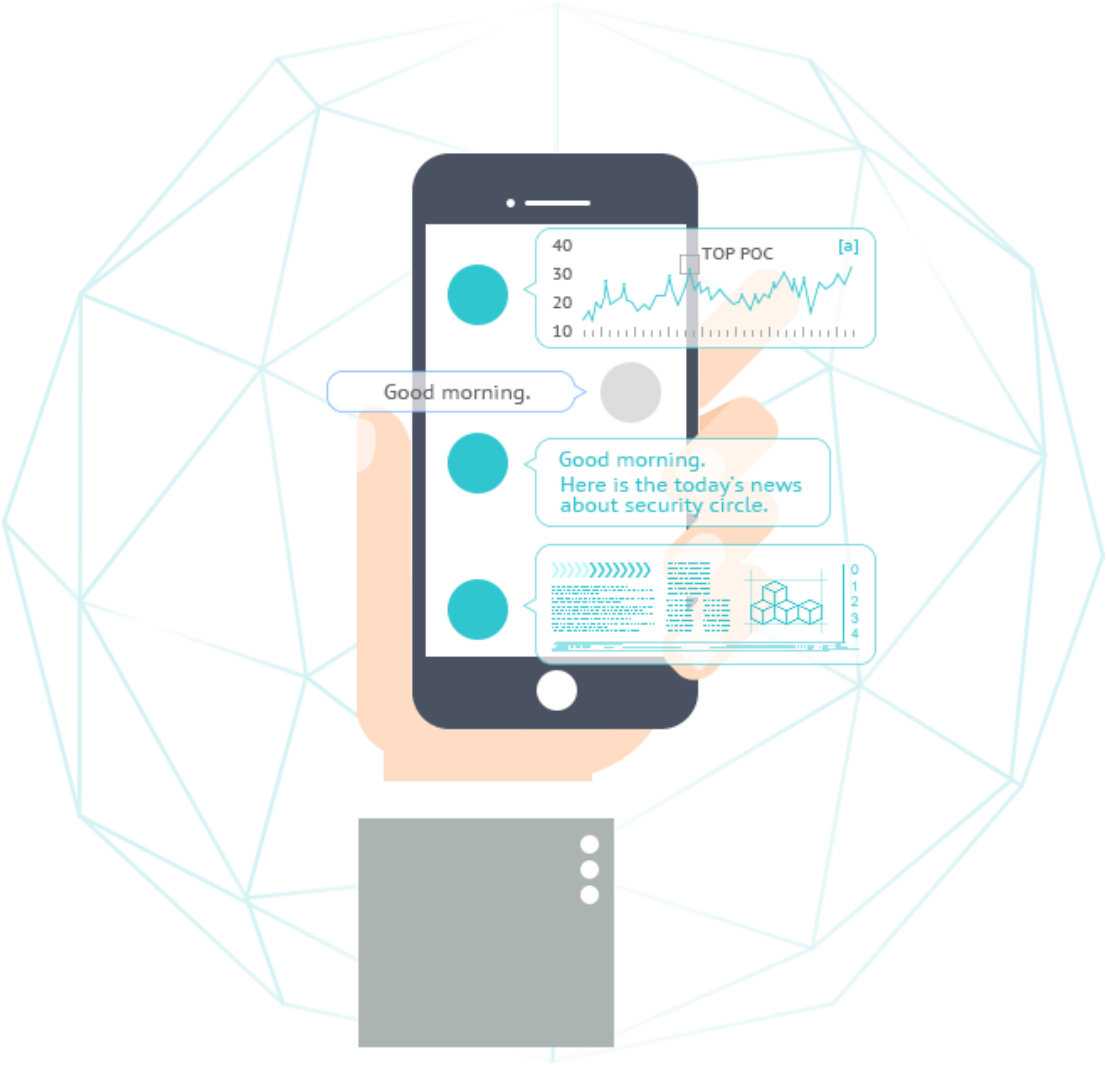
11.3.5.3. 报告制作

渗透测试之后会提供一份网站渗透测试报告，报告将会十分详细的说明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测试环节的操作。并且对于验证后信息进行人工分类及解决方案编写，根据专业工具扫描及人工验证结果，编制渗透测试报告。

11.3.5.4. 远程讲解

交付网站安全体检报告后，安全专家针对报告中的细节对客户进行内容讲解，告知客户体检报告重点内容及加固方案。

11.4. 漏洞速递服务内容说明



11.4.1. 漏洞速递

每日向客户推送当日最新漏洞信息、加固方案和信息安全新闻，对互联网上的信息安全新闻进行人工整理，将有价值的新闻通过微信企业号推送给客户。最新漏洞推送和每日安全新闻推送服务以年为周期。

11.4.2. 微信企业号推送

通过关注”知道创宇漏洞速递服务”企业号，可以更高效的接收和处理推送内容、文档归类以便于日后查阅。

11.4.3. Seebug 漏洞支持

知道创宇建立的 Seebug 社区是一个以收集、分享、处理安全漏洞为主的研究探讨类社区，通过采购漏洞速递的对应可选包，用户可以在 Seebug 社区查询自己想要了解的漏洞信息。Seebug 支持团队将在漏洞发布后对客户提供第一手漏洞情报及技术支持。

11.5. 网站监控服务内容说明

11.5.1. 站点可用率监控

“站点监控”包括多种监控类型，它们的共同特点是通过特定标准网络协议对网站或服务器进行外部监控，这些类型包括：

- 网页/HTTP，针对指定 URL 的网页
- Ping，针对服务器
- DNS，针对域名 DNS 解析
- FTP，针对 FTP 服务器
- SMTP，针对邮件 SMTP 服务器
- TCP，针对指定端口的 TCP 服务
- UDP，针对指定端口的 UDP 服务

客户可以根据需要来选择不同的监控类型，创建多个站点监控项目。比如：

需要监控 4 个网址，那么就可以创建 4 个网页/HTTP 类型的站点监控项目

需要监控 6 台服务器，那么就可以创建 6 个 Ping 类型的站点监控项目

无论采用哪种监控类型，都可以获得可用率报告和响应时间报告等。

11.5.2. 服务器性能监控

服务器性能监控是指针对服务器系统的运行状态以及各项指标的监控，支持 Linux/Unix 服务器以及 Windows 服务器的多项性能指标，包括：

- CPU 使用率
- CPU 负载
- 内存使用率
- 磁盘空间使用率
- 磁盘 I/O
- 网络流量
- 系统进程数

11.5.3. 网页性能管理

网页性能管理是对页面综合性能的全面监控、分析与优化，通过“页面性能指数”、“页面响应时间”和“可用率”3 项关键指标帮助客户了解网页综合性能，通过曲线图、饼图、柱状图、瀑布图等可视化方式查看数据，通过对页面元素的分析，指出页面存在的问题提出解决方案，为客户优化站点提供有力依据。

11.5.4. 告警通知

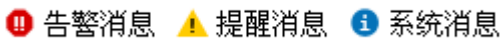
告警消息是给用户发送的站内消息，它包括以下几种类型：

- 故障消息：由网站或服务器自身问题引起的严重故障，导致服务中断时，您便会收到故障消息。比如网站无法打开、服务器 PING 丢包率为 100%，

服务器连接超时等。

- 提醒消息：当您设置了自定义告警线后，一旦触发，您便会收到提醒消息，比如服务器 CPU 使用率超过 90%、服务器网卡流量超过 5Mbps。
- 系统消息：对于服务器 SNMP 性能监控、服务性能监控、自定义监控，当采集器无法获取性能数据时，会记录系统消息，这时候您需要进行相应的检查，比如 SNMP 服务是否正常。

不同类型的告警消息图标如下：



网站监控服务支持以下几种告警通知方式：

- Email
- 手机短信
- RSS
- 电话语音

11.6. 输出报告

专业渗透测试完成后的两个工作日内，网站安全体检人员将输出最终版网站渗透测试报告。网站渗透测试报告包含网站渗透测试的整个流程描述，同时，还会对发现安全问题的思路与技术手法进行必要的说明，并结合测试目标所处的业务环境，对安全问题进行风险分析（如：可能产生的后果等方面）。

除此以外，测试人员还将针对发现的问题提出具有针对性的解决方案，以便用户在修复过程中参考使用。

12. 安全服务承诺

为提高安全服务质量，保证安全服务规范，知道创宇信息技术有限公司特做如下安全服务承诺：

1) 一切安全测试、评估类活动，均遵循国家法律、以及甲乙双方所约定的合同及补充条款要求；
2) 所有执行项目遵循双方约定服务范围；
3) 对于可能造成危害的测试行为提前获得用户同意与认可，并在双方约定的可控范围内进行测试；
4) 服务人员在整个测试过程中，将遵循内部规范严格规避可能存在的风险和隐患；
5) 测试结果按双方约定形式，由服务人员撰写报告完整提供给甲方，并按用户要求对内容做出适当的说明；
6) 在服务过程中，若因为人工失误造成的系统运行异常，测试人员有责任第一时间通知用户并协助恢复；
7) 乙方遵循安全保密要求，服务过程中和服务完成后，均不会以任何形式将服务过程中所获取的甲方数据泄露给第三方。

13. 常用工具

9.1 漏洞扫描与检测

编号	工具名称	网址
1	知道创宇 WebSOC plus	NA
2	Nessus	http://www.tenable.com/products/nessus
3	Acunetix Web Vulnerability Scanner	http://www.acunetix.com/vulnerability-scanner/
4	Nmap	http://nmap.org
5	Nikto	http://cirt.net/nikto2
6	Wapiti	http://sourceforge.net/projects/wapiti/
7	Oscanner	http://www.cqure.net/wp/oscanner/
8	Oracle Assessment Kit (OAK)	http://www.vulnerabilityassessment.co.uk/oak.htm
9	Oracle Auditing Tools (OAT)	http://www.cqure.net/wp/test/

9.2 漏洞利用工具

编号	工具名称	网址
1	Metasploit	http://www.metasploit.com/
2	The Exploit Database	http://www.exploit-db.com/
3	Perl	http://www.perl.org/
4	Python	http://python.org/
5	THC-Hydra	http://www.thc.org/thc-hydra/
6	SMBCrack	N/A
7	Absinthe	http://www.0x90.org/releases/absinthe

8	SQLMap	http://sqlmap.sourceforge.net/

10.渗透测试服务的特点

知道创宇是国内最早提出网站安全云监测及云防御的高新企业，始终致力于为客户提供基于云技术支撑的下一代 Web 安全解决方案。可以保证为客户提供先进、可靠的网站渗透测试服务。

- 工程经验：知道创宇已经对多个国家机关、互联网公司、新闻媒体成功的提供过网站安全体检服务，具有丰富的工程实施经验。
- 技术能力：自创立以来，知道创宇业绩卓著，得到了各大互联网管理机构、多家世界五百强企业的高度认可。2009 年公司被亚洲 CIO 杂志评选为 20 家最有价值企业，中国地区仅有知道创宇与阿里巴巴获此殊荣。知道创宇卓越的解决方案覆盖众多行业领域，拥有极高的客户忠诚度，这完全得益于精湛的技术、合理的总拥有成本、产品的易管理性以及优质的客户服务。
- 信息控制：网站安全体检项目成员对客户信息有着严格的信息控制手段及安全保密意识培训，保证客户的敏感信息的安全性。
- 人工筛查准确通告：基于知道创宇公司成熟的技术团队和强大的安全信息获取能力，会在发现漏洞的第一时间将漏洞信息发送至客户。同时，还会附有完整的漏洞加固方案及验证程序，帮助客户第一时间解决高风险漏洞。
- 互联网 APP 消息推送：漏洞速递的推送方式不同于以往的邮件、电话等告知方式，使用“微信企业号”进行消息推送。客户通过移动终端上的 APP 推送，可以第一时间获取漏洞信息、安全解决方案及验证程序。并通过 APP 收集、处理这些资料。随时随地，不遗漏重要信息。
- 漏洞获取能力：知道创宇的专业漏洞社区 seebug 为漏洞速递服务提供技术支持，seebug 专业漏洞社区成立于 2006 年，致力于打造一个良好的漏洞生态圈。通过 10 年的积累，seebug 社区获得了深厚技术实力和圈内人员的广泛支持。为了仅一步提升知道创宇的漏洞获取能力，在 Kcon 2015 黑客大会上，知道创宇正式向外发布了全新的 Sebug 漏洞社

区计划，鼓励技术人员踊跃到 Seebug 平台提交漏洞、PoC 等技术材料。依托于团队的专业技术实力和“互联网力量”的帮助，漏洞获取和解决能力非常强。

- 闭环处理流程和服务定制化：知道创宇的漏洞速递服务包含了从发现漏洞、验证漏洞和漏洞解决方案支持的全流程技术支持。客户可以通过漏洞解决方案自行处理漏洞加固问题，在实施过程中遇到的技术问题，知道创宇可以提供远程技术咨询。同时，客户可以选择知道创宇的应急响应服务，针对特定问题提供现场应急响应，依靠知道创宇强大的技术能力及丰富的项目经验，帮助客户解决技术难题。

11.知道创宇 KSA-sec 团队介绍

这是一支几乎从未在公众场合出现过的团队，他们是知道创宇为 VIP 用户打造的高级安全团队。和出现在乌云、补天、Seebug 等平台的漏洞团队不同，该团队仅针对高端客户作私属漏洞挖掘，并严格为其保守秘密。

这是由纯粹仅进行漏洞挖掘和攻击测试的知道创宇顶级安全专家构建的团队，他们和众测等由信息安全爱好者组成的社区不同，他们每个人都签署了严格的保密协议，并具备极高的职业素养，用户可放心的将业务系统交给他们进行测试。

KSA-sec 团队永远保持沉默，它仅对尊敬的客户进行点对点的贴心服务。

北京总部地址 :北京市朝阳区阜安西路望京 SOHO 中心

T3-A 座-15 层