46 | 安全第一：渗透测试

2018-10-12 茹炳晟

讲述：茹炳晟
时长 16:26 大小 7.53M

你好，我是茹炳晟。今天我和你分享的主题是：安全第一之渗透测试。

随着互联网的发展，网络环境越来越复杂，各类软件涉及的领域也越来越多，这时系统与软件的安全问题就愈加重要了。各类隐私信息、财务信息等的泄露，稍有不慎就会造成难以挽回的损失。

所以，大多数的公司，尤其是中大型的公司，已经针对系统与软件的安全采取了很多手段。比如，安装杀毒软件、定期给系统打补丁、定期进行漏洞及安全扫描、测试并封杀应用自身的安全漏洞等等。

虽说这些措施已经可以防止大部分的安全漏洞了，但却还不足以完全保证系统的安全性。这个时候，渗透测试便以其独立的“风姿”出现在了你我的视野里。

那么，接下来我们就一起看看什么是渗透测试，以及具体如何执行渗透测试吧。

渗透测试的定义

渗透测试指的是，由专业安全人员模拟黑客，从其可能存在的位置对系统进行攻击测试，在真正的黑客入侵前找到隐藏的安全漏洞，从而达到保护系统安全的目的。

或许你会有这样的疑问，软件系统在研发阶段已经用了各种手段保证安全性，为什么还需要进行渗透测试呢？

其实，这就好比让开发人员自己做测试一样，虽说他们对自己一手开发出来的软件产品再熟悉不过了，但却也是最难测出漏洞的。因为，开发人员的惯性思维，会使得他们在面对很多的潜在问题时，都误以为这不是问题的，所以我们需要引入独立的测试人员。

同样的道理，面对自己开发的系统，开发人员总是习惯性地去处理比较容易出现安全漏洞的地方，而对于一些隐藏的、不容易被发现的漏洞，却很难发现。

另外，**除了惯性思维之外，开发人员通常并不是安全领域的专家，因此往往会缺少专业的安全知识，不了解常用的系统攻击手段，从而导致他们并不能对安全相关的场景进行充分、客观的测试。**

这里，为了便于理解，我们可以将软件系统比喻成一座房子。

当房子建好后，我们会为其配备防盗门、防盗窗，甚至是安全警报器等，这时我们自认为这个房子足够安全了。但，我们永远都不知道，意图侵入者会使用什么样的方式找到漏洞从而攻克我们布置的安全防线。

所以，为了保证这座房子足够安全，我们会考虑聘请外部的安全专家来进行一系列的检测。比如，检测防盗门是否足够牢固、门锁是否容易被破坏、报警器是否在发生异常时能够正常发出警报、窗户和通道是否容易被侵入，或者从根本上判定我们所布下的安全防线，在安全机制上是否存在系统性的问题，以及需不需要更新等等。

我们甚至可以找人模拟入侵这座房子，在这个模拟过程中，由其发现这所房子是否还存在安全漏洞，以此验证房子真实的安全性。

那么，这个由外部的安全专家验证房子安全性的过程，便可以说是对这座房子进行渗透测试的过程。其中，这个房子便是我们的软件系统；而我们为验证房子安全性采取的这一系列方法，就是我们所说的安全渗透测试。

渗透测试的常用方法

那么，安全渗透测试应该怎样进行呢？在这里，我总结了渗透测试的五种常用测试方法，包括：

有针对性的测试；

外部测试；

内部测试；

盲测；

双盲测试。

接下来，我们就一起看看，具体每种测试方法，要如何开展吧。

1. **有针对性的测试**

有针对性的测试，是由公司内部员工和专业渗透测试团队共同完成的。其中，公司内部员工不仅要负责提供安全测试所需要的基础信息，同时也要负责业务层面的安全测试；而专业渗透测试团队，则更多关注业务以外的、更普适的安全测试。

有针对性的测试，属于研发层面的渗透测试。参与这类测试的人员，可以得到被测系统的内部资料，包括部署信息、网络信息、详细架构设计，甚至是产品代码。

有时，我们也把这种测试方法叫作“开灯”测试。之所以称为“开灯”测试，是因为有针对性的测试，是在测试人员完全了解系统内部情况的前提下开展的，有区别于外部人员完全不知道系统内部细节而进行的渗透测试。

2. **外部测试**

外部测试，是针对外部可见的服务器和设备（包括：域名服务器（DNS）、Web 服务器或防火墙、电子邮箱服务器等等），模拟外部攻击者对其进行攻击，检查它们是否能够被入

侵，以及如果被成功入侵了，会被入侵到系统的哪一部分、又会泄露多少资料。

一般情况下，外部测试是由内部的测试人员或者专业渗透测试团队，在假定完全不清楚系统内部情况的前提下开展的。

3. **内部测试**

内部测试是由测试工程师模拟内部人员，在内网（防火墙以内）进行攻击，因此测试人员会拥有较高的系统权限，也能够查看各种内部资料，目的是检查内部攻击可以给系统造成什么程度的损害。

所以，内部测试是为了防止系统的内部员工对系统进行内部攻击，同时以此来制定系统内部员工的权限管理策略。

4. **盲测**

盲测，指的是在严格限制提供给测试执行人员或团队信息的前提下，由他们来模拟真实攻击者的行为和上下文。通常，测试人员可能只被告知被测系统公开的信息，而对系统细节以及内部实现一无所知。

因为这种类型的测试可能需要相当长的时间进行侦察，所以代价会相对昂贵。而且，这类测试的效果，将在很大程度上取决于测试人员的技术水平。一般来讲，盲测是由专业渗透测试团队在测试后期开展的，通常会借助很多黑客攻击工具。

可以想象，如果测试人员拥有专业黑客的技术水平，同时结合各类渗透和黑客工具，一定能发现安全漏洞；但是，如果测试人员并不具备专业的安全测试以及系统攻击知识，那么可想而知，他们能够发现的问题就非常有限了。

5. **双盲测试**

双盲测试比盲测更进一步，也叫作“隐秘测试”。

在这类测试中，不光测试人员对系统内部知之甚少，而且被测系统内部也只有极少数人知道正在进行安全测试。因此，双盲测试可以反映软件系统最真实的安全状态，能够有效地检测系统在正常情况下，对安全事件的监控和处理能力是否合格。

因此，双盲测试可以用于测试系统以及组织的安全监控和事故识别能力，及其响应过程。一般来说，双盲测试一般是由外部的专业渗透测试专家团队完成，所以实际开展双盲测试的项目并不多。

执行渗透测试的步骤

了解了渗透测试的常用方法，那么到底要怎样具体开展呢？现在，我就和你分享一下开展渗透测试的 5 个主要步骤：

第一步：规划和侦察。这一步包含了定义测试的范围和目标、初步确定要使用的工具和方法、明确需要收集的情报（例如，网络和域名，邮件服务器），以更好地了解目标的工作方式及其潜在的安全漏洞。

第二步：安全扫描。安全扫描包括静态分析和动态分析两个阶段。

> 静态分析阶段，是通过扫描所有代码来估计其运行时的方式。这里，我们可以借助一些工具来一次性地扫描所有代码。目前，主流工具有 Fortify SCA 和 Checkmarx Suite。
>
> 动态分析阶段，则是在代码运行时进行扫描。这样的扫描更能真实反映程序的行为，可以实时提供应用程序的运行时视图，比静态扫描更准确、实用。

第三步：获取访问权限。在这一步，测试人员将模拟黑客对应用程序进行网络攻击，例如使用 SQL 注入或者 XSS 跨站脚本攻击等，以发现系统漏洞。然后，利用找到的漏洞，通过升级自己的权限、窃取数据、拦截流量等方式了解其可能对系统造成的损害。

至于到底什么是 SQL 注入，什么是 XSS 跨站脚本攻击，你可以自行查阅一些资料，也可以给我留言一起讨论。

第四步：维持访问权限。这个阶段的目的是，查看被发现的漏洞是否可以长期存在于系统中，如果漏洞能够被持久化，那么在很长的一段时间内入侵者都可以对系统进行深入访问或进行破坏。

这个阶段模仿的是高级持续性威胁。这类威胁，通常在系统中可以存在数月之久，入侵者可以借此获取组织内较高级别的敏感数据。

第五步：入侵分析。完成以上的四步之后，我们就要分析得到的结果了。通常情况下，我们需要将测试结果汇总成一份详尽的测试报告，并详细说明：

可以被利用的特定漏洞；

利用该漏洞的具体步骤；

能够被访问的敏感数据；

渗透测试人员能够在系统中不被侦测到的存在时间。

专业的安全人员会分析这些信息，以指导和帮助我们配置企业的 WAF(Web Application Firewall)，同时提供对其他应用程序的安全解决方案，以修补安全漏洞并防范未来的恶意攻击。

渗透测试的常用工具

目前，在实际的渗透测试中，我们通常会使用大量的工具来完成测试。为此，我挑选了 Nmap、Aircrack-ng、SQLmap、Wifiphisher、AppScan 这五种常用工具，和你分享一下它们的功能，以及适用的场景。

这里需要特别注意的是，这些工具本身就具有黑客属性，所以很多杀毒软件会阻止该类软件的运行。同时，你也一定不要在非官方的网站下载和使用这类工具，以防被意图不轨的人预先注入了危险的攻击点，请务必小心。

1. **Nmap**

Nmap 是进行主机检测和网络扫描的重要工具。它不仅可以收集信息，还可以进行漏洞探测和安全扫描，从主机发现、端口扫描到操作系统检测和 IDS 规避 / 欺骗。

Nmap 这类工具是渗透测试过程中最先要用到的，用来获取后续渗透测试过程中需要用到的系统基本信息，比如 IP 和端口等。

同时，Nmap 适用于各大操作系统，包括 Windows、Linux、OSX 等，因此是一款非常强大、实用的安全检测工具。

2. **Aircrack-ng**

Aircrack-ng 是评估 Wi-Fi 网络安全性的一整套工具。它侧重于 WiFi 安全的领域，主要功能有：网络侦测、数据包嗅探、WEP 和 WPA/WPA2-PSK 破解。

Aircrack-ng 可以工作在任何支持监听模式的无线网卡上并嗅探 802.11a、802.11b、802.11g 的数据。

Aircrack-ng 的执行是通过命令行或者脚本文件的方式，并且可以运行在 Linux 和 Windows 操作系统上。它的典型应用场景，主要包括数据包注入重播攻击、解除身份验证、虚假接入点等，也可以用于破解 WEP 和 WPA PSK。

3. **sqlmap**

sqlmap 是一种开源的基于命令行的渗透测试工具。它能够自动进行 SQL 注入和数据库接入，并且支持所有常见并广泛使用的数据库平台，包括 Oracle、MySQL、Microsoft SQL Server、SQLite、Microsoft Access、IBM DB2、FireBird、Sybase 和 SAP Max DB 等，使用的 SQL 注入技术也几乎涵盖了所有的攻击手段。

如果你不采用 AppScan 这类全面的商用安全测试工具，我的建议是通过 sqlmap 来确保系统数据库的安全性。

4. **Wifiphisher**

Wifiphisher 是一种恶意接入点工具，可以对 WiFi 网络进行自动钓鱼攻击。

渗透测试执行人员，可以通过 Wifiphisher 执行有针对性的 WiFi 关联攻击，轻松实现无线客户端的渗透测试。

Wifiphisher 还可以用于对连接的客户端进行受害者定制的网络钓鱼攻击，用来获取凭证（例如，从第三方登录页面或 WPA/WPA2 预共享密钥）或用恶意软件感染受害者站点。

5. **AppScan**

AppScan 是 IBM 公司的一款企业级商业 Web 应用安全测试工具，采用的是黑盒测试，可以扫描常见的 Web 应用安全漏洞。

AppScan 的工作原理是：

首先，从起始页爬取站下所有的可见页面，同时测试常见的管理后台；

然后，利用 SQL 注入原理测试所有可见页面，是否在注入点和跨站脚本攻击的可能；

同时，检测 Cookie 管理、会话周期等常见的 Web 安全漏洞。

AppScan 的功能十分强大，几乎涵盖了目前所有已知的攻击手段，而且攻击库还在不断地升级更新。此外，从 AppScan 的扫描结果中，我们不仅可以看到扫描的漏洞，还提供了详尽的漏洞原理、修改建议、手动验证等。

可以说，AppScan 是目前最完美的渗透测试商用解决方案，但是其最大的问题在于其价格昂贵，一般只有中大型的企业才会购买使用。

渗透测试的收益

现在，你已经清楚了开展渗透测试的必要性，也大致清楚了具体要如何开展渗透测试。那么，接下来，为了让你对开展渗透测试的信心更足，我再为你总结一下它能解决的问题：

通过渗透测试，公司可以识别出主要漏洞，并决定修补漏洞的优先级，同时合理分配系统补丁安装的时间，以确系统环境的安全性。

避免了安全漏洞，也就是避免了不必要的损失。因为，从安全漏洞中恢复出来，公司往往要花费巨大的代价去补救公司和客户的损失，甚至可能因此吃官司。而，渗透测试能够很好地避免这类问题，帮助公司树立良好的企业形象，因此赢得更高的信任度。

总的来说，我们应该按需选择适合自己产品的渗透测试方案，期间需要考虑到产品安全隐患和执行渗透测试的成本之间的平衡。

总结

在今天的这次分享中，我介绍了与渗透测试相关的知识点。

首先，渗透测试是指由专业安全人员模拟黑客，从其可能入侵的位置对系统进行攻击测试，以达到在真正的黑客攻击之前找到隐藏的安全漏洞，从而保护系统安全的目的。

然后，我根据发起渗透测试的位置以及对系统信息的掌握程度，将渗透测试分为了有针对性的测试、外部测试、内部测试、盲测和双盲测试这五种。

接着，我和你分享了开展渗透测试的 5 个步骤，分别包括了规划和侦察、安全扫描、获取访问权限、维持访问权限，以及入侵分析。

最后，我给你汇总了五款常用的渗透测试工具，其中功能最强大的要数 IBM 的 AppScan 了，但是其价格比较昂贵，适用于中大型企业。而关于如何选择适合自己的渗透测试方案，我的建议还是要综合考虑产品安全隐患和执行渗透测试的成本。

思考题

你所在的公司或者团队是否开展了渗透测试？你们会使用哪些渗透测试工具呢？

感谢你的收听，欢迎你给我留言一起讨论。

上一篇　45 | 打蛇打七寸：精准测试

下一篇　47 | 用机器设计测试用例：基于模型的测试

精选留言 (8)

写留言

Mark8287
2018-10-31

7

感谢作者的讲解，如果每篇文章下面有相关或推荐的资源就好了，比如渗透测试有哪些学习网站，资源等，谢谢。

红娟
2018-10-12

2

打卡 扩展了测试的视野，现在公司的产品都安全加密这一个特殊模块和相关认证。

小老鼠
2018-12-01

1

对于一个中小型企业而言，安全测试需要配置安全测试工程师吗？另外安全工程师与安全测试工程师区别在哪儿？

口水窝
2019-05-23

没有进行渗透测试，以前觉得安全测试，比如登录加密测试，就属于安全测试了，现在看来和渗透测试相差甚远，甚至不是一个概念，所以，持续学习，学以致用，才是我们最终目的。

展开

Alice
2019-01-25

茹老师，介绍渗透测试时，可以介绍下具体的测试案例，测试工具及测试工具的测试原理么？谢谢

作者回复: 用得最多的就是appscan

SimonWong
2018-11-03

滴滴，打卡。

展开

⃠b b
2018-10-13

渗透测试哦~ interesting

展开

涅槃Ls
2018-10-12

打卡46

展开