渗透测试：利用攻击者的思维方式保护关键资产

利用犯罪分子使用的工具、技术和实践识别关键漏洞

IBM Security

IBM

目录

执行概要

随着有价值数据的数量以及旨在保护此类数据的监管法规的数量不断增加，保护企业免遭网络犯罪的攻击变得更加重要。在 IBM X-Force Red 于 2017 年 8 月至 2018 年 11 月期间执行的 183 次渗透测试中，共确定了 1,099 个漏洞，其中 12% 的漏洞排名较高或非常关键。[1] 即便犯罪分子能够利用这 12% 的漏洞中的一个漏洞，就可能会对企业造成不利影响。

首席信息官、首席信息安全官和负责保护企业网络安全的其他高管经常会发现，识别和修复关键漏洞是一项艰巨的挑战。网络威胁针对的是组织内外的网络、硬件、应用、设备和员工。结合渗透测试结果， X-Force Red 认为 50% 的系统损害原因是由于密码强度较弱或采用默认密码及硬编码凭证所致。在 2017 年 10 月至 2018 年 11 月期间，该团队共向客户组织发送了 1,176 封网络钓鱼电子邮件；198 人点击了其中的链接，196 人提交了有效凭证。[2]

由于应对此类威胁的预算、资源和时间有限，一些组织选择使用自动化工具来测试他们的环境。然而，这些工具并非是为了发现未知威胁而设计的，而这些未知威胁往往是侥幸成功的"漏网之鱼"。

手动渗透测试旨在发现组织环境中最关键的已知漏洞和未知漏洞。从网络、应用、硬件及其他系统到 ATM、汽车、飞机、物联网设备等等，均可以进行渗透测试。越来越多的组织开始认识到手动测试的价值。举例来说，要求 X-Force Red 进行 ATM 测试的银行百分比从 2017 年到 2018 年增加了 300%。[3] 渗透测试可以帮助组织在产品设计期间及以后确立安全性、维持与监管标准的合规性并保护敏感数据。

与渗透测试需求相关的安全挑战

出于若干原因，企业中安全漏洞的数量在不断激增。公司未能遵循最佳安全实践，并允许员工、承包商和供应商无限制地访问其所有资产。无论资产的重要程度如何，也无论访问它们的角色如何，都会发生这种访问。更复杂的是，比以往任何时候都更具价值的数据会在网络、设备、应用和人员之间流动，而其中大部分数据都位于业务部门的孤岛中。这种复杂的基础架构使得组织难以了解其最重要的资产中的威胁和漏洞。

此外，威胁的类型也非常多样化，从犯罪集团到民族国家，从单独的"攻击者"到恶意和非恶意内部人员，都可能是攻击者。许多犯罪分子正在使用比以往更复杂的工具、技术和实践，悄悄绕过安全控件并诱骗相关人员释放敏感数据。

总测试次数	发现的漏洞总数	关键和高风险漏洞
183 次	1,099 个	136 个

图 1. 在 2017 年 8 月至 2018 年 11 月期间进行的 183 次测试中，X-Force Red 发现了 1,099 个漏洞。在这些漏洞中，有 136 个漏洞 (12%) 是高风险或关键漏洞。[4]

监管要求也增加了数据保护的压力和复杂性。举例来说，《支付卡行业数据安全标准》(PCI DSS) 设定的安全要求适用于处理支付卡交易的任何组织。无论交易的规模或数量如何，此类别中的每项业务都必须在一定程度上确保与 PCI DSS 的合规性。

另一项法规是《一般数据保护法案》(GDPR)，该法规要求组织保护欧洲数据主体的个人数据和隐私。如果违反 GDPR 的规定，组织的违规成本将会高达 2,000 万欧元或全球年营业额的 4%（以较高者为准）。

日常业务压力也会造成漏洞。货物和服务的周转及市场交付如果期限紧迫，也会优先于数据安全。合并和收购可能会导致公司在重组期间继承更多的数据缺陷。

鉴于这些因素，希望主动进行数据保护的企业应考虑纳入渗透测试。

渗透测试有何作用？

渗透测试是指模拟攻击和漏洞利用，旨在揭示特定目标的安全漏洞。利用犯罪分子可能用来攻入并破坏有价值资产的工具、技术和实践来执行这些测试。

渗透测试可以在内部或外部进行。该过程会评估访问敏感数据、利用系统缺陷的可能性。测试结果分为关键、高、中或低四个风险等级。其中关键或高风险事件很可能会损害系统，而不仅仅是存在理论威胁。

通过渗透测试，组织可以了解哪些资产易受攻击、存在哪些类型的漏洞。渗透测试人员能够展示犯罪分子利用漏洞的方式。然后，测试人员可以帮助组织在犯罪分子找到这些漏洞之前对其进行修复。进攻性交互有助于组织领先于犯罪分子。

通过渗透测试，用户有机会跳出漏洞扫描的局限性。扫描会发现已知缺陷，但可能会错过犯罪分子通过多个漏洞进行攻击的情况。犯罪分子也可能利用未知的技术手段逃避扫描检测。扫描可能会与某些系统和硬件组件不兼容。手动测试可以帮助检测扫描漏掉的漏洞。

通过内部团队进行渗透测试本身具有一定的局限性。如果测试团队规模不大的话，检测关键漏洞所需的测试数量可能会让他们不堪重负。安全团队可能不了解其他类似企业的攻击威胁，因为他们唯一关注的是他自身所在的组织。人员流失和技能短缺也会妨碍内部团队在攻击防范方面的效率。

外部渗透测试团队几乎可以进行任何方面的测试。他们会结合手动测试和自动化工具，以提高已知漏洞和未知漏洞的查找效率。这种团队也更容易扩展，因为他们的团队规模更大，也拥有更多的专业知识。外部渗透测试团队也能够更广泛地了解威胁情况，因为他们会为许多组织执行测试。通常而言，这些组织也有自己的研究团队和威胁情报来源。

此外，许多内部测试团队不具备汽车、物联网设备和 ATM 等领域的专业知识，因此在这些领域同样采用计算机领域测试时所用的方式。这些垂直行业需要特定的测试专业知识、技术和工具，而这些只有外部渗透测试团队可以提供。

IBM 的解决方案：IBM X-Force Red 渗透测试服务

IBM Security 的 X-Force Red 渗透测试服务能够为客户提供他们所需的技能和规模，帮助他们找到并修复最危险的漏洞。X-Force Red 团队包括有数百名白帽黑客，他们在渗透攻击方面拥有数十年的丰富经验，使用与犯罪分子相同的工具、技术、实践和思维方式。经验丰富的专家和开发人员了解如何构建代码和设备，以及攻击者针对它们实施攻击的方式。在临时或订阅服务中，X-Force Red 团队使用的测试方法包括虚拟或现场手动测试和自动扫描。

使用 X-Force Red 渗透测试服务的客户几乎涵盖了各个行业的大型国际企业和小型公司。无论企业规模大小，X-Force Red 团队都可以为其测试任何网络、应用、硬件、人员或设备。无论是在产品开发期间还是上市后，该团队均可对产品进行测试。X-Force Red 已经为数百家组织进行了渗透测试，而且这一数量还在不断增加。

X-Force Red 团队使用类似于“礼品卡”的形式销售其服务。作为其订阅服务的一部分，客户每月支付固定费率，而且可随时更改他们想要测试的内容。测试的持续时间取决于环境的大小及受测区域，例如代码行数。

咨询服务可以帮助客户确定最适合其需求的测试种类。在测试结束时，X-Force Red 团队会提交一份报告，其中会列明调查结果、所用的方法和补救建议。通过该报告，客户可以了解可能会对其业务产生最大影响的严重漏洞，以及如何快速修复这些漏洞。

X-Force Red 团队可以测试应用、网络、人员、硬件等。该团队还可以测试 ATM、汽车以及嵌入式设备和物联网设备。

应用测试

应用是许多企业的核心。如果关键应用出现故障，业务运营也会停止。

为了保护应用安全，一些组织依赖于自动化安全控件。但是，这些控件只能解决自动化攻击。只有人才能发现并解决人工手动攻击。

还有一些组织会使用应用防火墙；不过，这些防火墙会遗漏逻辑缺陷，即：应用正在做什么以及为什么这么做，而犯罪分子经常会绕过并利用这些缺陷实施攻击。此外，应用可能包含有恶意软件，而恶意软件一旦安装，就可能会感染组织的系统。

X-Force Red 团队在 2018 年 8 月至 11 月期间为各组织进行了 24 次应用测试。测试结果如下图所示：

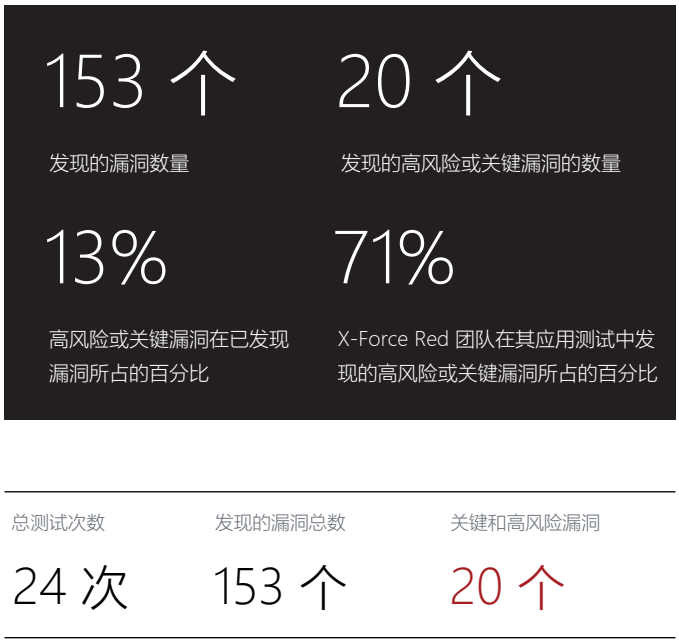

图 2. 在应用测试方面，从 2018 年 8 月到 11 月共进行的 24 次测试，发现了 153 个漏洞。在这些漏洞中，有 20 个测试（13% 的测试）发现了高风险漏洞或关键漏洞。

为了缓解这些缺陷，X-Force Red 团队会对应用进行手动测试，以识别安全流程和控件中开发人员可能忽略的漏洞。测试人员还会验证已知漏洞和"尚未知"漏洞并消除误报。

X-Force Red 团队还会执行应用源代码审查。客户可以提供其源代码，以节省测试时间、提升成本效益。

越来越多的董事会开始要求进行应用安全测试，因为关键应用是保持业务运行的决定因素。与此同时，越来越多的行业合规性法规也开始要求进行渗透测试，例如 PCI DSS。X-Force Red 应用测试可帮助客户满足合规性要求，并在应用上市之前和之后建立安全性。

网络测试

使用来自第三方供应商的技术可能会使公司网络面临风险。供应商可能会不遵守安全策略和程序。公司可能会在不遵循最佳安全实践的情况下安装这些技术。

此外，一些公司可能不会对内部通信或网络上其他应用进行加密。由于存在这些缺陷，犯罪分子就可以破解密码并访问公司的服务器、虚拟机、客户数据、数据库备份等。

X-Force Red 团队可以通过手动网络渗透测试帮助组织识别这些问题。该评估服务会从网络的角度衡量设备的安全性，重点关注公开的服务、配置和基础架构。此类测试能够确定犯罪分子可能会实施的机会性攻击，以及扫描程序可能无法检测到的漏洞。

X-Force Red 测试人员使用与犯罪分子相同的工具、技术、实践和思维方式攻入组织的网络基础设施，以识别其中存在的漏洞。该团队能够识别缺陷，例如网络主机是否与另一个易受攻击的主机建立了活跃的信任关系。测试通常会在员工使用网络的工作时间进行，并且可以在需要快速修复时立即予以响应。测试项目通常需要一到两周的时间，具体取决于网络规模。

通过网络测试，客户可以了解如何通过程序化更改，加强整个网络及整个基础架构的保护。网络测试还可以帮助安全领导人了解投资重点，以最大限度地降低风险。

人员测试

虽然越来越多的公司开始开展安全意识培训，但仍有一些公司根本没有对员工进行培训，或者培训的频次非常低。即使是最好的安全管制也无法阻止针对员工的一些攻击。

如前所述，X-Force Red 发现，密度强度不够或使用默认密码和硬编码凭证是导致被攻击的主要原因。另一个挑战是打击网络钓鱼攻击，即犯罪分子发送电子邮件说服员工泄露个人信息。

X-Force Red 团队使用社交工程手发来制造类似犯罪分子使用的诡计。测试人员会分析哪些人员与恶意电子邮件进行了互动。他们还会进行钓鱼攻击或语音钓鱼演练，查看员工会通过电话向未经证实的个人泄露哪些敏感信息。

其他测试包括使用加载了虚假内容的 USB 并诱使用户插入设备。在物理安全测试方面，X-Force Red 团队会通过尝试访问公司的安全区域及敏感信息来评估安全策略和程序。即便是像一盒甜甜圈一样简单的东西，都可能会让 X-Force Red 的白帽黑客得到攻入的机会。

测试结束时，X-Force Red 团队会提供经过优先排序定制化的建议列表，以帮助组织规避已识别的漏洞。

硬件测试

试图破坏设备的犯罪分子通常很少会遇到障碍。他们可以购买相同型号的设备，然后攻入设备内部，发现其中的漏洞并借助这些知识来挖掘将会暴露目标的缺陷。许多硬件设备不会对存储的数据进行加密，而且在生产期间，还会在设备上留下功能信息。犯罪分子可以找到某一种型号的设备，检索默认凭证并使用相同的凭证破坏目标设备。

X-Force Red 测试人员会审查产品从始至终的构建方式。此类测试针对的是所有电子设备，以及构成设备一部分的外壳。X-Force Red 测试人员还会帮助选择和实施部件和管制，以便在产品中构建安全性，而不是进行事后安全补救。

X-Force Red 团队提供两种类型的硬件测试。第一种是"白盒"测试：客户提供设计文档、源代码和设计原理图。X-Force Red 团队审查流入和流出系统的源代码和数据，并识别产品实现和外部库中的漏洞。第二种是"黑盒"测试，X-Force Red 团队对产品进行反向工程，以重新创建设计文档。此过程会测试产品在整个生命周期中的漏洞，包括源代码和实现。

ATM、物联网和汽车特定测试

X-Force Red 团队在 ATM、汽车、物联网、销售点和其他设备的测试方面拥有数十年的丰富经验。该团队测试人员专注于针对如何保护这些系统的研究和测试，以及在设计期间及以后提供指导。X-Force Red 团队会全面了解这些系统的缺陷和漏洞，并在需要时提供实际操作帮助。

我们以 ATM 为例。ATM 无处不在，里面存有数千美元的现金，无时无刻不在吸引着犯罪分子。

从 2018 年 1 月到 10 月，X-Force Red 团队发现 ATM 的最大安全问题是缺乏全盘加密、机柜锁不够安全。有一名测试员在 20 秒内就破坏了 ATM 机柜锁。

银行认识到这些威胁的严重性，如下图所示：

300%

从 2017 年到 2018 年要求 X-Force Red 团队进行 ATM 测试的银行数量增加了三倍。单单是在亚太地区，ATM 测试请求就增加了五倍。

之所以出现大幅增加，部分原因是由于联邦调查局发布了关于 ATM"兑现"攻击泛滥的警告。下图说明了这种威胁：

FBI 警告：兑现攻击

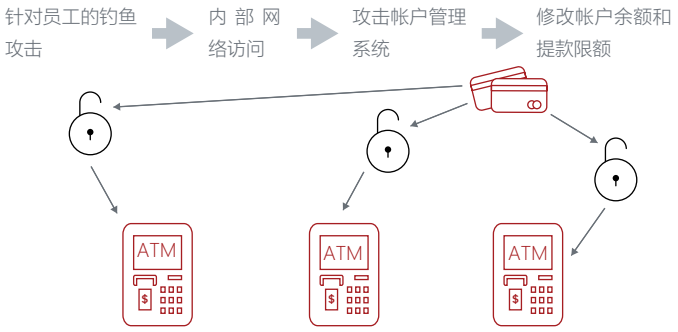

图 3. 在"兑现"攻击中，犯罪分子会操纵提款限制并伪造欺诈性 ATM 卡取现，最终可能会支取客户账户中的所有资产。

X-Force Red 团队能够为客户提供现场 ATM 测试、虚拟测试和其他测试选项。客户也可以将 ATM（以及物联网和汽车特定的设备及类似电子设备）运送到 X-Force Red 实验室进行测试。

X-Force Red 在美国德州奥斯汀、佐治亚州亚特兰大、英国赫斯利及澳大利亚墨尔本设立了 4 个实验室。在实验室内，测试人员会拆解特定的硬件设备以识别缺陷。他们还会评估硬件的构成、与软件的互动以及相关事项。X-Force Red 测试人员还会建立产品目标，建立安全要求并模拟威胁，以发现漏洞。他们可以帮助公司在产品投放市场之前修复安全漏洞，以避免潜在的财务损失和品牌损害。

X-Force Red 门户

X-Force Red 门户能够为客户提供方便、直接和受保护的通信，还能够让他们与测试人员开展协作。借助该门户（一个基于云的平台），客户可以采用加密形式请求测试。客户随时可以直接通过该门户联系测试人员，提出问题或意见，这就避免了交换电子邮件和电话。

X-Force Red 门户还有助于实现更快的实时修复。传统的方式是测试人员在项目结束后一到两周内编写报告。这种事件滞后意味着客户必须等待测试结果，这就会让犯罪分子有更多的时间进行攻击，同时还可能会出现新的漏洞。借助 X-Force Red 门户，测试人员可以在识别到漏洞后第一时间提交结果，以便客户能够快速查看和修复漏洞。该门户可提供测试进度和结果的单个视图，以便客户和测试人员了解彼此的情况。

输入到该门户的交互式报告中包含有关于漏洞的主要测试结果、漏洞利用证据以及漏洞优先排序和补救方面的详细指导。在将报告输入到该门户时，X-Force Red 允许安全领导人确定哪些人员有权查看测试结果。客户可以进一步细分报告的各个部分，进而限制个人只能看到其授权范围内的漏洞。在整个过程中，确定整个组织修复程序的权限一直都由安全领导人控制。

X-Force Red 门户可以看做是面向客户的所有报告的中央存储库。执行多项测试的组织可以实时监控、跟踪和审查所有报告。客户会收到一份历史记录，以便比较发现的缺陷以及所做的改善。

该门户还有自己的安全管制，包括安全套接字层（SSL）、加密、双因子认证等。

结语

由安全漏洞引发的潜在诉讼、财务损失和品牌损害的数量不断激增，这意味着组织需要积极主动地保护其最宝贵的资产。借助 IBM X-Force Red 渗透测试服务，客户可以在犯罪分子利用漏洞之前识别并修复关键漏洞。X-Force Red 测试人员使用与犯罪分子相同的工具、技术和实践，而且在识别和利用漏洞方面拥有数十年的经验。由于 X-Force Red 测试人员采用与攻击者相同的思维方法，因此能够找出犯罪分子可能都没有尝试过的新方式来攻击组织。总而言之，借助 X-Force Red 渗透测试服务，组织可以找出并修复其基础架构中的关键缺陷，进而能够制定安全管制、加强安全措施，确保始终领先于犯罪分子。

有关更多信息

如欲了解有关渗透测试的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：ibm.com/security

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国印刷
2019 年 1 月

本文档截至最初公布日期为最新版本，IBM 可随时对其进行修改。IBM 并不一定在开展业务的所有国家或地区提供所有这些产品或服务。

本文所讨论的性能数据是基于特定操作条件得出的。实际结果可能会有所差异。本文档内的信息"按现状"提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有任何关于适销性、适用于某种特定用途的保证以及不侵权的保证或条件。IBM 产品根据其提供时所依据的协议的条款和条件获得保证。

客户应负责确保与适用法律和法规的合规性。IBM 并不提供法律建议，亦不声明或保证其服务或产品可确保符合任何法律或法规。

良好的安全实践声明：IT 系统安全涉及通过对来自贵企业内外部的非法访问进行阻止、检测和响应来保护系统和信息。非法访问会导致信息变更、损毁、盗用或滥用，或导致对您的系统的破坏或滥用，包括用于对他人的攻击。没有任何 IT 系统或产品可被视为完全安全，也没有单一产品、服务或安全措施可完全有效地阻止非法使用和访问。IBM 系统、产品和服务设计为合法、全面的安全方法的一部分，该方法必然涉及其他操作程序并可能需要其他系统、产品或服务，以达到最大效力。IBM 不保证任何系统、产品或服务可免受，或使贵企业免受任何一方的恶意或非法行为的影响。

1. X-Force Red 渗透测试结果，2017 年 8 月至 2018 年 11 月。
2. X-Force Red 渗透测试结果，2017 年 10 月至 2018 年 11 月。
3. X-Force Red ATM 渗透测试，2018 年 11 月。
4. X-Force Red 渗透测试结果，2017 年 8 月至 2018 年 11 月。

17023217-CNZH-00