XCTF

第1章 渗透测试技术基础

《Metasploit渗透测试指南》

目录 content

目录 content

0x01：PTES标准中的渗透测试阶段

XCTF

定义：

用来定义渗透测试过程，并确保客户组织能够以一种标准化的方式来扩展一次渗透测试，而无论是由谁来执行这种类型的评估。

阶段：

- 前期交互阶段
- 情报搜集阶段
- 威胁建模阶段
- 漏洞分析阶段
- 渗透攻击阶段
- 后渗透攻击阶段
- 报告阶段

0x01：PTES标准中的渗透测试阶段

前期交互阶段：

前期交互阶段通常是由你与客户组织进行讨论，来确定渗透测试的范围和目标。这个阶段最为关键的是需要让客户组织明确清晰地了解渗透测试将涉及哪些目标。而这个阶段也为你提供了机会，来说服客户走出全范围渗透测试的理想化愿景，选择更加现实可行的渗透测试目标来进行实际实施。

- 与客户组织讨论
- 确定渗透测试的范围和目标

0x01：PTES标准中的渗透测试阶段

XCTF

情报搜集阶段：

在情报搜集阶段，你需要采用各种可能的方法来搜集将要攻击的客户组织的所有信息，包括使用社交媒体网络、Google Hacking技术、目标系统踩点等等。而作为渗透测试者，你最为重要的一项技能就是对目标系统的探查能力，包括获知它的行为模式，运行机理，以及最终可以如何被攻击。对目标系统所搜集到的信息将帮助你准确地掌握目标系统所部属的安全控制措施。

- 社交媒体网络、 Google Hacking技术、目标系统踩点等等
- 获知目标系统的行为模式、运行机理

0x01：PTES标准中的渗透测试阶段

威胁建模阶段：

威胁建模主要使用你在情报搜集阶段所获取到的信息，来标识出目标系统上可能存在的安全漏洞与弱点。在进行威胁建模时，你将确定出最为高效的攻击方法，你所需要进一步获取到的信息，以及从哪里攻破目标系统。在威胁建模阶段，你通常需要将客户组织作为敌手看待，然后以攻击者的视角和思维来尝试利用目标系统的弱点。

- 标识出可能存在的安全漏洞与弱点
- 确定攻击方法

0x01：PTES标准中的渗透测试阶段

漏洞分析阶段：

一旦确定出最为可行的攻击方法之后，你需要考虑你该如何取得目标系统的访问权。在漏洞分析阶段，你将综合从前面的几个环节中获取到的信息，并从中分析和理解哪些攻击途径会是可行的。特别是需要重点分析端口和漏洞扫描结果，攫取到的服务“旗帜”信息，以及在情报搜集环节中得到的其他关键信息。

- 分析端口和漏洞扫描结果，服务“旗帜”信息等关键信息
- 得出可行的攻击途径

0x01：PTES标准中的渗透测试阶段

XCTF

渗透攻击阶段：

渗透攻击可能是在渗透测试过程中最具魅力的环节，然而在实际情况下往往没有你所预想的那样“一帆风顺”，而往往是“曲径通幽”。最好是在你基本上能够确信特定渗透攻击会成功的基础上，才真正对目标系统实施这个渗透攻击，当然在目标系统中很可能存在着一些你没有预期到的安全防护措施，使得这次渗透攻击无法成功。但是要记住的是，在你尝试要触发一个漏洞时，你应该清晰地了解在目标系统上存在这个漏洞。

- 前几个阶段中对漏洞信息和漏洞利用方式的研究是关键
- 可能存在预期之外的安全防护措施

0x01：PTES标准中的渗透测试阶段

XCTF

后渗透攻击阶段：

后渗透攻击阶段在任何一次渗透测试过程中都是一个关键环节，而这也是能够体现出你和那些平庸的骇客小子们的区别，真正从你的渗透测试中为客户提供有价值信息情报的地方。后渗透攻击阶段将以特定的系统为目标，识别出关键的基础设施，并寻找客户组织最具价值和尝试进行安全保护的信息和资产，当你从一个系统攻入另一个系统，你需要演示出能够对客户组织造成最重要业务影响的攻击途径。

- 识别关键基础设施，寻找最具价值的信息和资产
- 得出能够对客户组织造成最重要业务影响的攻击途径

0x01：PTES标准中的渗透测试阶段

报告阶段：

当你在编写和报告你的发现时，你需要站在客户组织的角度上，来分析如何利用你的发现来提升安全意识，修补发现的问题，以及提升整体的安全水平，而并不仅仅是对发现的安全漏洞打上补丁。

- 至少分为摘要、过程展示和技术发现
- 技术发现是体现渗透测试价值的位置，充分考虑导致漏洞的原因后，给出修补建议

目录 content

0x02：渗透测试类型

根据客户组织在渗透测试前提供的信息量划分

- 白盒测试
- 黑盒测试
- 灰盒测试

0x02：渗透测试类型

白盒测试

- 客户组织的IT支持和安全团队提供目标系统的全部信息
- 测试过程不会被客户的安全团队阻断
- 时间有限，或情报搜集等环节不在测试范围内的时候适用
- 无法测试目标系统的应急响应程序和安全防护计划的效果

0x02：渗透测试类型

黑盒测试

- 模拟攻击者的入侵行为进行测试
- 测试者需要自行搜集目标系统的情报
- 能够测试安全团队的检测和防御能力
- 不需要找出所有漏洞，以找出并利用可以获取目标系统访问权代价最小的攻击路径为目标，并保证不被检测到

0x02：渗透测试类型

灰盒测试

- 白盒测试的目标系统信息量+黑盒测试流程和技术手段
- 与黑盒测试相比，扩展了攻击面
- 能够发现内部用户可能的攻击方式
- 测试过程中与目标客户进行沟通，有助于删除一些无意义的发现，和确认具有重要意义的发现

目录 content

0x03：漏洞扫描器

- 通过获取目标系统的操作系统指纹信息来判断其类型与版本，以及上面所运行的所有服务
- 使用漏洞扫描器执行一些特定的检查，来确定存在着哪些安全漏洞
- 检查例程的质量取决于他们的开发者，很多时候会漏掉或是错误标识系统上的安全漏洞
- 从漏洞扫描器中获取到的知识可能是非常有价值的，但小心不要过分地依赖它们

XCTF

Thanks for watching 谢谢