如何学习渗透测试：初学者教程

原创

网络安全进阶 于 2019-08-25 12:25:39 发布 9693 收藏 173
分类专栏： 渗透测试 文章标签： 渗透测试 渗透测试教程 学习渗透测试 web安全测试 新手入门

本文链接：https://blog.csdn.net/fengzheng126/article/details/100061920

**

本文首发于公众号：乌云安全，提供关于渗透测试、社会工程学、黑产的技术及资讯，关注该公众号福利多多。

**

免责声明：黑客攻击是一项难以学习的技能。只需做一些在线课程，你就不会成为一个好的笔友。只需安装Kali Linux并学习如何使用这些工具，你就不会成为一名优秀的测试者。这是一条充满挑战的道路，无尽的挫折感，你不会在一天 - 一个月 - 甚至一年内学会如何旅行。但是，如果你有决心，你会发现它是一个非常有益的领域，你可能永远不想离开。
在本教程中，我将具体介绍 渗透测试的Web应用程序黑客攻击 方面。这是道德黑客攻击的指南。如果你做的是那种不道德的事情，请尽早放弃。

假设知识：
基本技术背景（Unix命令，一些软件开发技巧）
强烈渴望打破局面

0 - 背景知识
一些CS101知识是必须的。试图学习如何在不熟悉Unix命令的情况下进行攻击，这不仅仅是试图在你走路之前跑步。这就像飞行A380而不知道朝哪个方向。

如果你试图在没有必要的知识储备的情况下进入渗透测试行业并且想随着时间的推移“填补知识空白”，那么你不必要花费太多时间考虑如何开始学习，以下是你需要了解的内容：

如何使用Linux：Linux / Unix用于编码和测试的主要功能来自终端和可用的工具数量。你可以试试在Windows中做你需要的一切，但这并不容易 - 如果你正在进行测试，你最终需要了解一些Linux。相信我：如果你找到一份安全工作，而你的同事发现你从未使用过Linux，他们会永远嘲笑你。
这里有三个主要选项：
安装Linux发行版（例如Ubuntu）。您最好的选择是下载一个虚拟机软件，您可以在其中包含Linux安装（下面的链接）。
如果你有的话，继续使用macOS。你可以凑合用这个，因为在Mac上的终端和工具几乎是一样的Linux操作系统。
在Windows 10上使用Ubuntu。我认为这对于初学者来说是最糟糕的选择，因为在安装工具时它可能非常不可靠，并且让GUI工作有时可能是一场噩梦。
VirtualBox：免费的虚拟机软件
Ubuntu：体面的Linux启动发行版
在VirtualBox中安装Ubuntu
初学者的Unix命令

如何编码：现在您已经设置了环境，我们可以获得有趣的一点！学习一些基本的编码技能对于测试是必不可少的。如果你想学习如何打破它，首先要学习如何制作它。对于Web应用程序测试，您将需要学习一些完整的堆栈内容，如
HTML，CSS，Javascript和Python。Python具有成为脚本编写的优秀语言的额外好处，并允许您编写自己的测试工具（令人兴奋！）。
学习前端
学习Python

1 - 设置您的环境

如果你是开发者，你可能已经拥有了完美的设置。格拉茨！这里的方式通常是Linux或Mac。就个人而言，我在Windows 10上使用Ubuntu（起诉我），但仅仅因为我知道我最喜欢的工具。
许多初学者都是从Kali开始的，但我建议不要这样做。成为一个自信的测试者的一部分是建立你的工具库。Kali递给你一堆工具，其中没有一个你真正理解和欣赏。

但无论你做什么，你都有一个舒适的设置是绝对至关重要的。现在花些时间来解决您在设置中可能遇到的任何问题（如引导加载程序，窗口管理器，GUI等）。当你拥有无数的窗户和复杂的工具时，Pentesting会变得混乱，你需要的最后一件事就是你自己的环境对你不利。

2 - 学习理论

没办法绕过这个。即使只是在网络应用程序中进行黑客攻击，也需要知道一整套知识。我将网络黑客知识分为两类：基础知识和Nifty技巧。基础知识是你应该首先从书籍，视频，在线教程等学到的东西。
不幸的是，鉴于黑客攻击的速度有多快，大多数有能力的网站已经安全地反对基础知识（但你仍然需要了解它们！）。Nifty Tricks是真正的赚钱人。稍后您将通过浏览经验丰富的pentesters博客，加入道德黑客社区以及模糊Youtube视频来了解这些内容。如果你是第一个发现Nifty Trick的人，你可以在名人堂获得一席之地，也许还有很多钱。

以下是基础知识的一些很好的资源：
Web应用程序黑客手册：这是一个很好的起点。这涵盖了您所需的几乎所有基础知识。但是不要为书中附带的“实验室”而烦恼。
OWASP的测试指南：OWASP是Web应用程序黑客攻击的关键参与者，本指南是巨大的。它有很多你需要知道的东西。
Youtube上的LiveOverflow：这个人很棒 - 他涵盖了很多基础知识以及大量的Nifty技巧。
Hacksplaining：关于不同漏洞的大量信息。
SecHub：一系列不同漏洞的汇编，也有写作！超酷。
了解HTTP TCP / IP模型，基本网络和数据包。你需要这个，相信我。

一旦你学习并练习了基础知识（更多关于如何在下一节练习），你可以继续学习一些Nifty技巧。一些资源：
DEF CON视频很棒。
漏洞撰写：有很多地方可以找到它们，而Medium可以是一个很好的地方。查看r / Netsec。谷歌还有一个漏洞，你想要了解更多关于附加单词“writeup”或“POC”的漏洞，例如“XSS writeup”。你会发现非常聪明的人发布的关于他们发现利用东西的新方法的帖子。
寻找测试社区并加入他们。令人惊讶的是，黑客攻击是一个非常社交的领域，只需与其他测试者交谈，就可以学到很多很酷的技巧。

3 - 练习CTF和战争游戏

这是有趣的一点。一旦你有一些理论失败，你可以通过做黑客挑战开始练习。这些是易受攻击的Web应用程序，具有通过利用应用程序找到的隐藏“标记”。
CTF（夺旗）比赛是记分牌和球队的现场比赛，而战争游戏竞争力较弱，更像是练习技能的游乐场。
查看当前和即将到来的CTF的CTFtime，尽管这些CTF对于初学者来说太难了。好的战争游戏是OWASP的WebGoat和OverTheWire。还可以查看OWASP的Juice Shop，Hacker101 CTF，Hack The Box和Google的XSS游戏。

虽然有趣并且是学习的好方法，但请注意，战争游戏/ CTF所需的技能与实际应用程序（如bug赏金）所需的技能略有不同。有可能成为CTF的最佳得分手，但完全无法做出错误赏金（这是我一段时间），反之亦然。
战棋是错误的恩泽什么Civ5是运行一个实际的国家（好吧，也许不是那么极端，但 有什么 的区别 时下？）。战争游戏教你一些优秀的策略和解谜技巧，但现实生活是一个不同的景观 - 更多关于这一点在第5节。

4 - 擅长脚本编写

这将使您的生活更加轻松。Python作为一种脚本语言令人惊叹，特别是对于黑客攻击。许多CTF和bug赏金都需要强力操作，例如发送许多数据包和散列，所有这些都可以通过编写自己的Python脚本轻松完成。

查看pwntools，一个Python CTF框架。它简化了漏洞利用写作！这是你发送数据包的方式。

我建议创建一个文件夹，保存自己的Python脚本并随着时间的推移在其上构建。我真的不能低估这将节省你多少时间。

5 - 真实世界和Bug赏金

在某些时候，您将获得第一次中等难度CTF挑战的标志，而无需谷歌解决方案。你会感到惊讶。可能，你花了几个小时和几个小时，最后自己找出答案将是一种感觉，让你永远迷上它。

你现在是个猎人。激烈。势不可挡。

你甚至可能认为你已经准备好开始赚钱了。但是一旦你查看bug赏金网站，你就会发现你不知道自己在做什么。没有线索告诉你漏洞在哪里。有一个如此广泛的攻击面，你甚至不知道从哪里开始。成千上万的黑客已经将网站清理干净了。

尽管它可能令人沮丧，但这才是真正开始的乐趣所在。你现在已经离开了操场，准备和大孩子一起玩。一个很好的起点是观看我之前链接的这个DEFCON视频，并挖掘寻找好工具和更多Nifty技巧。

现在是开始学习网络侦察的时候了。它在DEFCON视频中得到了很好的体现，在构建您的侦察工具库时，您将了解更多相关信息。

6 - 了解你的工具

工具不会成为黑客。但如果没有它们，你可能不会太过分。

我建议首先下载一些常用工具，如Nmap和BurpSuite。Nmap是一种发现工具，可以在域上查找主机和开放端口，通常可以让您对网络的外观有一个良好的感觉。BurpSuite是您最好的朋友，这是网络黑客的第一个多功能工具。它的主要用途是捕获和编辑数据包，但它确实可以做更多的操作。

在这两个之后，你可以找到（或制作）最适合你的工具。以下是我的一些最爱：

Sublist3r：我非常喜欢这个子域名枚举器。这很疯狂，发现了很多东西。

Aquatone：与Sublist3r类似，但更强大。我通常先运行Sublist3r，然后将Aquatone保留在后台。

dirsearch：目录bruteforcer。

LinkFinder：发现Javascript文件中的端点。

recon-ng：一个完整的网络侦察框架，可以完成所有工作。

SecLists：本身不是一个工具，而是一系列用于强制执行的列表。几乎是网络测试的主要内容 - 我几乎把它放在强制性部分。

Spotify黑客混合带感觉很酷

7 - 继续黑客攻击

我告诉过你这很难，不是吗？

Pentesting具有挑战性，令人困惑，总体而言令人沮丧。但如果你真的想做这件事，你就会找到克服所有这些的方法。

尝试加入社区，例如Twitter和Bugcrowd上的社区。

请记住：这是一个非常重要的领域，也是未来非常有前景的领域。