热榜：2015年度渗透测试神器TOP 10

小太阳花 2015-10-09

现在，安全研究者对网站或者应用程序进行渗透测试而不用任何自动化工具似乎已越来越难。因此选择一个正确的工具则变得尤为重要，正确的选择甚至占去了渗透测试成功半壁江山。

如果你在网络上搜索渗透测试工具，你会找到一大堆，其中不乏付费的、免费的、商业的以及开源的。但是，热门的测试工具都有哪些呢？这里我们将为大家梳理出2015年度十大最佳渗透测试工具。

之所以强调是本年度的，这点尤为重要，因为研究者使用的工具年复一年的都在发生着变化。

Metasploit——独一无二，不可取代

Metasploit自2004年发布以来，以迅雷不及掩耳之风席卷网络安全界。这是一个用于开发、测试以及漏洞EXP代码的先进开源平台。其可扩展模型包括生成payloads、解码器、无作业生成器以及EXP，这使Metasploit框架成为尖端渗透研究的一个重要途径。它同时附带了数以百计的EXP，你能够从模块列表中看到它们。这样一来编写EXP将变得更加轻松，同时它还能将那些互联网黑暗角落中可疑的非法shellcode一网打尽。还有Metasploitable，一个免费的虚拟系统，专为测试Metasploit以及其他EXP工具而开发的特意不安全Linux虚拟系统。

w3af——带你破解网站

w3af是一个非常受欢迎、强大并且灵活的框架，用于寻找并利用web应用程序漏洞。它的运用和拓展都十分简便，并且具有几十个web评估和利用插件。从某些方面来看，它就像一个聚焦于web的Metasploit。

Core Impact——想玩渗透，请付钱吧！

Core Impact可并不便宜（准备花费至少3万美金），但是它被广泛认可是最强大的可用漏洞利用工具。它运行着一个巨大并且定期更新的专业EXP数据库，同时可以完成一些小奇招，例如EXP一台机器然后通过那台机器建立一个加密通道，再挖掘其他盒子。当然，其他一些不错的选择，像是Metasploit和Canvas。

SQLMap——学习SQL注入

SQLMap是一个开源渗透测试工具，能够自动检测、利用SQL注入漏洞，以及接管数据库服务器。它有一个强大的检测引擎，提供渗透测试人员很多细分的特性。一系列功能开关，从数据库指纹识别，即从数据库读取数据到识别操作系统，通过外带传输连接在操作系统远程执行命令。

Canvas——吾爱0day利用

Canvas是一个来自Dave Aitel ImmunitySec公司的商业漏洞利用工具。它包括超过370个EXP，并且比我们之前介绍的Core Impact或者Metasploit商业版本更为便宜。它还附带了完整代码，以及一些0day漏洞。

Social Engineer Toolkit——呵呵哒，愚蠢的人类

Social Engineer Toolkit（SET）工具在一个接口囊括了许多有用的社会工程学攻击。SET的主要目的是自动化并改进社会工程学攻击。它能够自动生成隐藏了EXP的网页或电子邮件消息，同时还能使用Metasploit的payload，例如网页一旦被打开便会连接shell。

sqlninja——检测SQL注入&征服一个网站

sqlininja使用Microsoft SQL Server作为一个后端数据库挖掘web应用漏洞。它聚焦于获取远程主机上正在运行的shell。起初，Sqlninja并不寻找SQL注入，而是在一个SQL注入被发现之后自动进行漏洞利用。

Netsparker——是个不错的工具

Netsparker是一个web应用安全漏洞扫描工具，可同时支持漏洞检测与利用，能够高效高准确率的检测SQL注入漏洞和XSS漏洞。一旦在成功进行漏洞利用或者其他测试之后再次报告确认的漏洞，它便会显示为假阳性。

BeEF——朋友，不要忘了它

BeEF是一个web框架攻击测试平台。这个工具可实时展示收集的僵尸浏览器以及浏览器漏洞。它为目标个体或者组织的僵尸浏览器提供了命令以及控制接口。

dradis——黑客通信工具

Dradis是一个开放源代码的框架，可以让渗透测试参与者在其中进行高效的信息分享。它自身包含了一个独立的Web应用程序，它提供了一个集中的资料库来记录什么迄今已完成的工作和仍然需要做的工作。它的用于读取和收集输出的插件

Dradis远远不只是一个单纯的记笔记的应用程序。它支持SSL通信，可以导入的Nmap和Nessus结果文件、附加文件、生成报表，并且可以扩展，通过扩展就可以与（如漏洞数据库）外部系统结合。

小结

不知道你最喜欢的工具是不是也在列表当中，如果没有请敲击你的键盘让我知道你还想在列表中添加什么工具以及原因！通过文章下方的评论，或许大家可以交流更多经验哟！

使用工具来实现你的计划，但是请不要用它们来搞破坏，让我们做一些有意义的事情，难道不好么？

***参考来源：EHACKING，编译/小太阳花，转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）**