> Christopher Hadnagy从事计算机技术14年之久，现在全心投入在计算机安全中“人”的研究。他成立了Social-Engineer.Com，致力于帮助公司提高安全性，并教授给他们“坏人”的做法。他研究并破解了最近发生的很多恶意攻击事件。他推荐的实践测试法被500强公司采用，用来教育员工安全方面的知识。你可以在www.social-engineer.org找到他。
>
> 译者/ 陆道宏

什么是社会工程？

我认为社会工程的真正定义是：一种操纵他人采取特定行动的行为，该行动不一定符合“目标人”的最佳利益，其结果包括获取信息、取得访问权限或让目标采取特定的行动。

社会工程有很多不同形式，既可以是恶意的，也可以是善意的，既可以具有激励作用，也可以具有毁灭性。社会工程人员也会有不同的目的和类型，他们可能是黑客、渗透测试者、间谍、身份窃贼、不满的员工、高明的骗子、高端猎头、销售人员、政府、医生、心理医生，甚至是律师。

信息收集是社会工程的一个关键方面。若在这一点上投入的精力不足可能会导致社工行动的失败。现在，社工人员可以通过多种工具来收集、分类以及运用这些数据信息。这些工具完全改变了社工人员查看和使用数据的方式。社工人员将不再局限于使用常规的搜索方式找寻数据，这些工具为他们打开了互联网的资源之门。

社工人员花费了大量时间来完善其自身的技能，然而，许多攻击方式需要通过创建附加恶意代码的邮件或PDF文档来实现。

这些事情都可以利用BackTrack中包含的诸多工具来手动完成。起初搭建www.social-engineer.org网站的时候，我曾和好友戴夫•肯尼迪（Dave Kennedy）交谈过。戴夫是流行工具FastTrack的开发者，FastTrack使用Python脚本和网页界面能够自动实现渗透测试中的许多最常用的攻击。我告诉戴夫单独为社工人员开发一个类似FastTrack的工具是个不错的主意，这个工具让社工人员点击几下鼠标就能创建PDF文件、电子邮件及网站等，这样就可将注意力集中到社会工程中的“社会”这部分上来了。

戴夫仔细思考了这个问题，决定创建一些简单的Python脚本，让社工人员可以创建附加恶意代码的PDF文件并随邮件发送。于是社工人员工具包（Social Engineer Toolkit，SET）就诞生了。在写本文的时候，SET已经被下载了超过150万次，而且很快成为社工人员进行审计时配备的标准工具包。本节介绍SET的主要特点及使用方法。

安装

安装步骤十分简单。前提是已经安装了Python和Metasploit框架。这两个软件在BackTrack发行版中已经存在，所以不用担心。BackTrack 4甚至已经包含了SET。如果需要从头开始安装，过程也十分简单。依据导航进入安装目录，在控制台窗口上运行如下命令：

```
svn co http://svn.secmaniac.com/social_engineering_toolkit set/
```

执行完命令之后，将得到一个名为set的目录，该目录下包含了所有SET工具。

运行SET

运行SET的过程也很简单。只需在set目录下输入./set，就会启动初始SET菜单。

请登录social-engineer.org网站，这里有SET菜单的完整展示图，以及对每个菜单选项全面、深入的介绍。接下来介绍SET中两个最常用的功能。

首先讨论鱼叉式网络钓鱼攻击，然后讨论网站克隆攻击。

鱼叉式网络钓鱼

网络钓鱼是一个术语，描述恶意诈骗犯如何通过定向设计的电子邮件“广泛撒网”，吸引人们访问特定的网站、打开恶意文件或者输入个人敏感信息，为以后的攻击做准备。要在今天的互联网世界生存，必须能够检测、防御此类攻击。

社工审计人员使用SET可以创建有针对性的电子邮件对客户进行测试，然后记录有多少雇员上当了。这个信息随后可用于培训，以帮助员工识别和避免这些陷阱。

使用SET进行鱼叉式网络钓鱼攻击，选择选项1。选择1后，会看到如下几个选项：

1. 执行群发邮件攻击
2. 创建一个文件格式负载
3. 创建一个社工模板

要进行邮件式钓鱼攻击，选择第一个选项。第二个选项用于创建一个恶意的PDF或其他文件，以备作为邮件附件发送。第三个选项用以创建模板，待日后使用。

在SET中发起攻击十分简便，只需选择正确的菜单选项然后点击启动。例如，如果我想发动邮件攻击，向受害者发送伪装成技术报告的恶意PDF文件，我会选择选项1——执行群发邮件攻击。

接下来，我会选择一个攻击向量（选项6），这种攻击对很多版本的Adobe Acrobat Reader软件都有效——应用了`Adobe util.printf() Buffer Overflow`[1]漏洞。

1 请参见http://www.nsfocus.net/vulndb/12573。——译者注

接下来几个选项会设置攻击的技术问题。点击选项2——Windows Meterpreter Reverse_TCP。使用Metasploit接收反向会话、或者受害者电脑的IP和端口，以避免入侵检测系统（IDS）或其他系统的报警。

选择443端口，使数据流看起来好像是加密的SSL数据。SET会创建恶意PDF文件并设置监听功能。

执行上述步骤后，SET会询问是否要更改PDF的文件名，例如改成类似TechnicalSupport.pdf等更加隐蔽的名称，然后输入邮件信息以备收发。最后，SET发出一封看起来很专业的电子邮件，引诱用户打开附件中的PDF文件。受害者收到的邮件如图1所示。

邮件发送之后，SET会创建一个网络监听器等待目标打开文件。一旦目标点击了PDF，监听器就会执行恶意代码，让攻击者得以进入受害者的计算机中。

真是惊人（也许有人并不这样认为），所有这一切只需点击六七下鼠标，审计者便可将精力集中在攻击的真正的社会工程方面了。

图1　一封无害的电子邮件与一个简单的附件

这是一个破坏性很强的攻击，因为它利用了客户端软件的漏洞，而且在大多数情况下，屏幕上不会显示有情况正在发生。

这只是应用SET可以发动的众多攻击中的一种。

Web攻击

SET也允许审计人员克隆任何网站并在本地运行。这种攻击类型的强大之处在于可以让社工人员以多种方式诱骗他人访问克隆网站并从中获利。社工人员既可以伪装成更新网站的开发者，也可以仅仅对网址进行细微的修改（填加或删除一个字母），最终诱使他人访问克隆的网站。

一旦有人访问了克隆网站，社工人员便可以发动多种不同的攻击，包括信息收集、证书收集和直接入侵等。

要在SET中运行此攻击可从主菜单中选择选项2（网站攻击），选择之后，可以看到以下几个选项：

1. Java Applet攻击方法
2. Metasploit浏览器的入侵模式
3. 证书获取的攻击方式
4. 标签绑架攻击方法
5. 中间人攻击方式
6. 回到前面的菜单

选项1中的Java Applet攻击是一种特别邪恶的攻击。一般情况下，Java Applet攻击会在用户界面上弹出一个Java安全警告，说该网站已被ABC公司签名，并让用户同意这一警告。

进行这种攻击，先选择选项1，然后选择选项2——网站克隆（Site Cloner）。

选择网站克隆的时候，需要输入你想克隆的网站地址。这里可以选择想克隆的任何网站——客户的官方网站、客户供应商网站或者政府网站。正如你所想象的，重点在于选择一个对目标有意义的网站。

在这个练习中，假设是克隆Gmail网站。屏幕上会显示如下信息：

```
SET supports both HTTP and HTTPS
Example: http://www.thisisafakesite.com
Enter the url to clone: http://www.gmail.com
[*] Cloning the website: http://www.gmail.com
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: DAUPMWIAHh7v.exe
[*] Malicious java applet website prepped for deployment
```

上述工作完成之后，SET会询问你想要在自己与被害者之间创造什么类型的连接。要想使用本书讨论的技术，选择Metasploit的反向会话界面，也就是Meterpreter。

SET为负载加密提供了多种选项，这是为了避开反病毒系统的检测。

下一步，SET启动内嵌的网站服务器为克隆网站提供服务，同时启动监听器准备捕获浏览该网站的受害者。

现在只需要社工人员构造一封电子邮件或给目标打个电话，让目标访问该假冒的网站。最后，用户会看到如图2所示的界面。

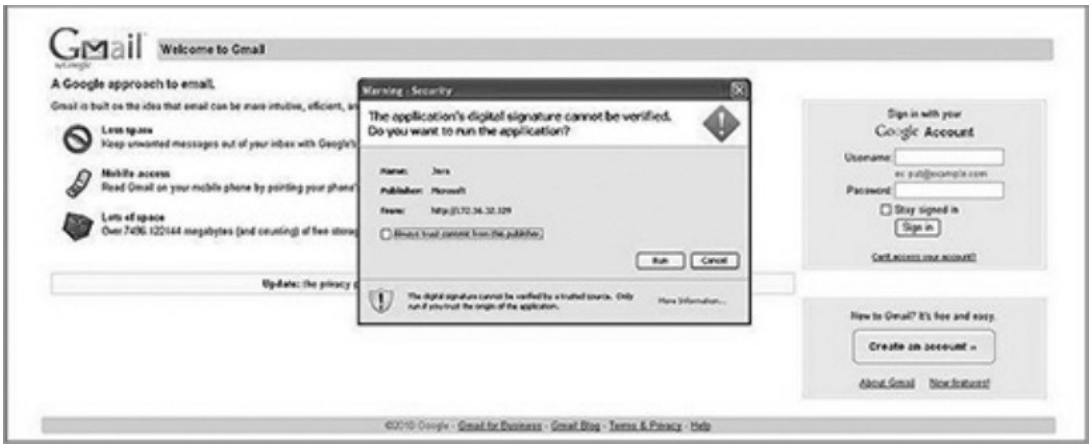


图2　谁会不相信微软签名的小程序呢？

最终结果是，一个Java Applet出现在用户面前，告诉他该网站已被微软签名，他需要允许安全证书运行，才能继续访问网站。

只要用户允许了该安全证书，攻击者就可以立刻入侵他的计算机了。

SET的其他特性

SET是具有实战思维的社工人员开发出来的，所以工具集所提供的都是审计过程中常常会用到的攻击方法。

SET在不断更新和发展。例如，最近几个月，除网站克隆和网络钓鱼攻击之外，SET又增加了一些其他的攻击方式，还增加了一个传染性媒体生成器。传染性媒体生成器允许用户创建带恶意文件的DVD、CD或USB，这

些传染源可以混杂在目标对象的办公大楼里。当它们被插入计算机时，将触发恶意负载程序的执行，从而开启受害人机器的入侵之门。

SET也能创建简单的负载和相应的监听器。如果社工人员想要通过一个提供反向会话功能的EXE可执行程序连接回他的服务器，可以在审计过程中携带一个U盘。如果面前的机器是他想要远程访问的，便可将U盘插入，导入负载文件，然后点击运行。这样可以在目标机器和他自己的机器之间建立起一个快速连接。

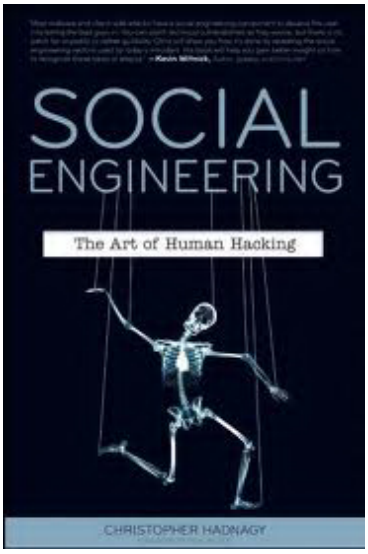
有一种较新的攻击方式叫Teensy HID攻击。Teensy设备是一个小的可编程电路板，可嵌入键盘、鼠标或其他可插入电脑的电子设备。

SET可对Teensy编程，设置这个小电路板在插入电脑时将执行何种命令。常见的命令包括创建反向会话或监听端口等。

SET的最新特性之一是提供了一个Web界面。这意味着SET会自动启动Web服务器程序，从而更易于应用。图3显示了这个网页界面的概貌。

SET是一款强大的工具，它能帮助社会工程审计人员测试出公司存在的常见弱点。SET工具的开发者总是善于听取他人的意见，在工具中增添新的应用，使得其不断完善、越来越流行。如果想更深一步了解这个强大的工具，可以登录http://www.social-engineer.org网站，上面包含每个菜单选项的详细说明。在使用过程中，可以通过http://www.social-engineer.org和http://www.secmaniac.com这两个网站对SET不断更新。

图3　SET的新Web界面



Social Engineering首次从技术层面剖析解密社交工程手法，介绍了社交工程的所有方面，包括诱导、假托、心理影响和人际操纵等，通过实际的例子、个人经验、及背后的科学，探讨和解释了社交工程的奥秘。本文选自Social Engineering。