[-] 新的set.config.py文件生成： 2016-10-25 22:11:39.751762

[-] 验证配置更新...

[\*]更新时间戳验证配置: 2016-10-25 22:11:39.751762

[\*] 设置是使用新的配置，无需重新启动

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

/ \_\_\_\_\_/\\_ \_\_\_\_\_/\\_\_ \_\_\_/

\\_\_\_\_\_ \ | \_\_)\_ | |

/ \ | \ | |

/\_\_\_\_\_\_\_ //\_\_\_\_\_\_\_ / |\_\_\_\_|

\/ \/

[---] The Social-Engineer Toolkit (SET) [---]

[---] Created by: David Kennedy (ReL1K) [---]

Version: 7.4.1

Codename: 'Recharged'

[---] Follow us on Twitter: @TrustedSec [---]

[---] Follow me on Twitter: @HackingDave [---]

[---] Homepage: https://www.trustedsec.com [---]

欢迎来到社会工程师工具包（组）。

一站式商店为您所有的需要。

Join us on irc.freenode.net in channel #setoolkit

社会工程师工具包是一个产品TrustedSec。

Visit: https://www.trustedsec.com

更新使用者的框架很容易！（PTF）

Visit https://github.com/trustedsec/ptf to update all your tools!

从菜单中选择:

1) 社会工程攻击

2) 渗透测试（快速轨道）

3) 第三方模块

4)更新社会工程师工具包

5)更新配置设置

6)帮助命令

99) 退出社会工程师工具包

选项 主菜单>1

从菜单中选择

1) 矛式网络钓鱼攻击向量

2)网站的攻击向量

3)传染介质发生器

4) 创建一个有效负载和侦听器

5) 大规模的邮件攻击

6)基于Arduino的攻击向量

7) 无线接入点攻击向量

8) 二维码生成器的攻击向量

9) PowerShell攻击向量

10) 短信欺骗攻击向量

11) 第三方模块

99) 返回主菜单。

选项主菜单>1 >1

的链接模块允许你特殊工艺的电子邮件发送给一个大（或小）附文件的恶意的有效载荷的人数。如果你想恶搞你的电子邮件地址，确保“发送邮件”是安装（apt-get install sendmail）和更改配置/ set\_config sendmail =了Sendmail =旗。

有两种选择，一是把脚弄湿，让设置为你做的一切（选项1），二是创建自己的文件格式的有效载荷和使用它自己的攻击。无论哪种方式，好的D运气和享受！

1)执行大规模电子邮件攻击

2) 创建一个文件格式的有效载荷

3) 创建一个社会工程模板

99) 返回主菜单

选项主菜单>1 >2

网络攻击模块是一种独特的方式，利用多个基于Web的攻击，以妥协的意图的受害者。

java applet的攻击方法将恶搞一个java证书将Metasploit的基于有效载荷。使用一个定制的java applet由Thomas Werth提供的有效载荷。

Metasploit的浏览器开发方法将利用浏览器漏洞通过选择Metasploit iframe将Metasploit的有效载荷。

凭据收割机方法将利用网络克隆的一个网站，有一个用户名和密码字段和收获所有的信息张贴到网站。

的tabnabbing方法将等待用户移动到一个不同的选项卡，然后刷新页面不同的东西。网络攻击方法介绍了顶管white\_sheep，emgent。该方法利用iframe的替换使突出显示的网址链接到合法的出现然而当点击弹出窗口U然后被替换的恶意链接。你可以编辑的set\_config链接替换设置如果太慢/快。

多攻击方法将通过Web攻击菜单添加一个组合的攻击。例如，你可以利用java applet，Metasploit的浏览器，凭据收割机/ tabnabbing一下子的EE是成功的。

HTA的攻击方法将允许你克隆一个网站通过hta文件可通过基于浏览器的Windows PowerShell开发执行PowerShell注射。

1) java applet的攻击方法

2) metasploit浏览器漏洞的方法

3) 凭证收割机攻击方法

4)tabnabbing攻击的方法

5)网络顶进攻击法

6) 多攻击网络方法

7) 全屏幕攻击法

8) HTA的攻击方法

99)返回主菜单

选项主菜单>1 >3

**感染的USB / CD / DVD模块**创建一个autorun.inf文件和Metasploit的有效载荷。当DVD / USB / CD插入，它会自动运行，如果自动启用。

选择你想使用的攻击向量：文件格式错误或直接执行。

1) 文件格式的成就

2) metasploit可执行标准

99) 返回主菜单

选项主菜单>1 >4

**创建一个有效负载和侦听器**

1) Windows Shell Reverse\_TCP 在受害者的命令外壳上产卵，并发送回攻击者 2) Windows Reverse\_TCP Meterpreter 出现在受害者的Meterpreter壳寄回给攻击者 3) Windows Reverse\_TCP VNC DLL 出现在受害者的VNC服务器并发送回攻击者 4) Windows Shell Reverse\_TCP X64 Windows x64的shell命令，反向TCP内联

5) Windows Meterpreter Reverse\_TCP X64 连接到攻击者（Windows x64），Meterpreter 6) Windows Meterpreter Egress Buster 产卵的Meterpreter壳和通过多个端口到端口的家庭

7) Windows Meterpreter Reverse HTTPS 在使用SSL和HTTP隧道通信使用Meterpreter

8) Windows Meterpreter Reverse DNS 使用主机名而不是IP地址，使用反向Meterpreter

9) Download/Run your Own Executable 下载一个可执行文件并运行它

选项主菜单>1 >5

社会工程师工具包 Mass E-Mailer

对大众来说有两个选项，首先会发送一封电子邮件给一个人。第二个选项将允许您导入一个列表，并将其发送到尽可能多的人，因为你想要的薄的列表。

你想做什么:

1. E-Mail 攻击单电子邮件地址

2. E-Mail 攻击邮件群发

99. 回到主菜单。

选项主菜单>1 >6

基于攻击向量利用arduin基于设备Arduino程序装置。你可以利用小小的、具有板载存储和可允许的物理远程执行代码L系统。由于设备注册为USB键盘会自动禁用或绕过任何端点的系统保护。

你将需要购买的USB设备，大约是22美元。这种攻击向量将自动生成所需的代码，以便为您部署系统上的有效负载。

这个攻击向量将创建。进口到Arduino必要PDE文件（用于编程的小小的IDE）。的攻击范围从基于PowerShell的下载者，名攻击，一和其他方法。

有关规范和良好的教程访问的更多信息:

http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle

购买的访问： http://www.pjrc.com/store/teensy.html

特别感谢：IronGeek，WinFang，Garland

这个攻击向量也攻击X10控制器，一定是这个利用X10的基础通信设备为了工作。

选择一个有效载荷创建PDE文件导入到Arduino:

1) PowerShell的HTTP GET MSF载荷

2) 名HTTP GET MSF载荷

3) Powershell 基于反向外壳的有效载荷

4) Internet Explorer/FireFox Beef Jack 有效载荷

5)去恶意java网站和接受程序的有效载荷

6) Gnome wget 下载有效载荷

7) 二进制2的攻击(MSF的有效部署)

8) SD卡2小小的攻击（部署任何exe）

9) SD卡2小小的攻击（部署在OSX）

10)X10 Arduino嗅探器PDE和图书馆

11) X10 Arduino干扰PDE和图书馆

12) PowerShell的shellcode的直接攻击

13)peensy多攻击DIP开关+ SD卡攻击

99)返回主菜单

选项主菜单>1 >7

无线攻击模块创建一个接入点，利用你的无线网卡和重定向DNS查询到你的所有。这个概念是相当简单的，将创建一个无线接入点，DHCP SErver，和恶搞的DNS流量重定向到攻击者的机器。它将退出该菜单，作为一个子进程运行的一切。

然后你可以开始任何你想设置的攻击向量，例如java applet的攻击，当受害者加入您的接入点和尝试去一个网站，将被重定向到攻击者的机器我。

这个攻击向量需要airbase-ng，AIRMoN NG，DNSSpoof，和dhcpd3。

1) 启动设置的无线攻击矢量接入点

2) 停止设置无线攻击矢量接入点

99)返回主菜单

选项主菜单>1 >8

QRcode的攻击向量将创建一个为您的任何URL你想要QRCode。

当你的QR码生成，选择在设置一个额外的攻击向量和部署的QR码到受害者。例如，生成一个QR码的java applet和发送二维码通过梅勒。

Enter the URL you want the QRCode to go to (99 to exit):

输入你想要的QR码到URL（99退出）：

选项主菜单>1 >9

PowerShell的攻击向量模块允许你创建PowerShell特定攻击。这些攻击将允许您使用PowerShell的所有Windows操作系统的默认可访问A及以上。PowerShell部署有效载荷和执行，不得由预防性技术触发功能提供了丰富的景观。

1) PowerShell的字母数字的shellcode注射器

2) PowerShell反向外壳

3)PowerShell结合壳

4) PowerShell Dump SAM 数据库

99) 返回主菜单

选项主菜单>1 >10

----- 社会工程师工具包（套）短信欺骗攻击向量 -----

这个攻击向量依赖于三分之一方服务称为www.spoofmytextmessage.com。这是三分之一方服务以外的控制，从社会工程师工具包。在一家的优秀的人oofmytextmessage.com有供我们使用，为了让集进行短信欺骗提供了一个未公开的API。你将需要访问https://www.spoofmytextmessage.com并注册一个ACC考虑。他们的例子多种付款方式如贝宝，比特币，和更多的选择。一旦你购买你的计划，你想要的，你将需要记住你的电子邮件地址和密码使用帐户帐户。然后设置将处理其余。

为了解决这个问题你必须有一个帐户，在spoofmytextmessage.com

特别感谢哈利勒@ sehnaoui测试服务为我找到spoofmytextmessage.com

[!] 免责声明: 提交的是的，你明白你接受所有条款和服务spoofmytextmessage.com你充分了解你的国家的法律立场，短信欺骗履行之前这些。通过接受是的，你完全承认这些条款，不会使用他们的非法用途。

你接受这些条件（是或否）:

选项主菜单>1 >11

[-] 社会工程师工具包第三方模块菜单。

[-] 请阅读自述/ modules.txt关于如何创建自己的模块。

1. Google Analytics Attack by @ZonkSec

99. 返回到前一个菜单

简单钓鱼网页：1232

需要映射的地址：

需要克隆的网址：