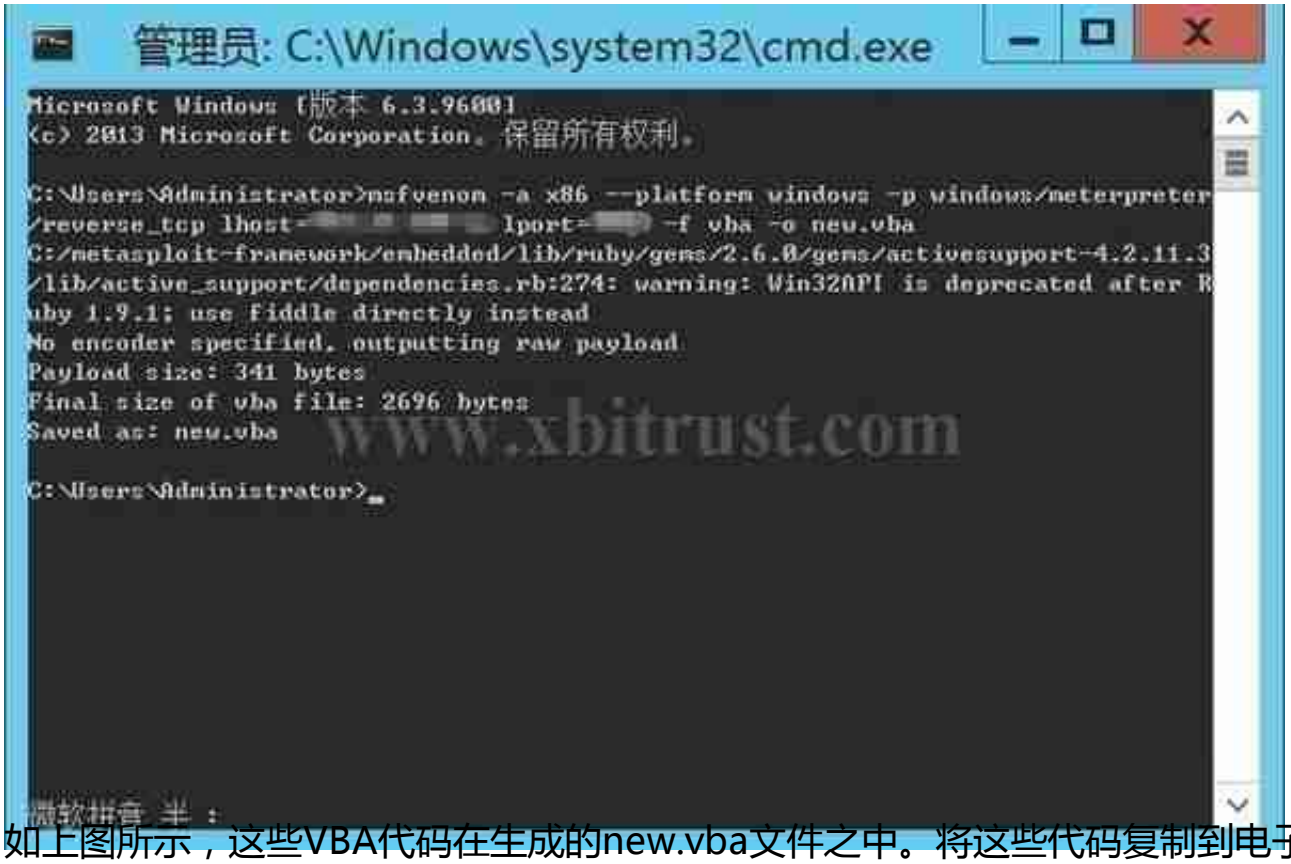
2、Web shell攻击实践

在获知用户ID和密码的情况下有多种方式可以获得完整或不完整的Cookie（包括手动登录网站，找到完整Cookie进行复制），而采用Python的Selenium模块一般可以获得完整的Cookie，以便程序登录我们的某自有网站。Selenium模块是一个用于Web应用程序测试的工具，它直接运行在浏览器中，就像真的用户在操作一样。在获得了完整的Cookie后，使用程序来进行各种操作就很便捷了。

编写一个简单的窃取Web服务器的多种环境信息的文件webshell.html，尝试使用程序或手动将其上传至某自有测试网站，这可借助该网站登录后可上传如头像之类的功能来实现。对于头像，由于按网站限制往往只能上传图像格式，因此先把待传文件的扩展名进行修改，例如改为webshell.jpg。

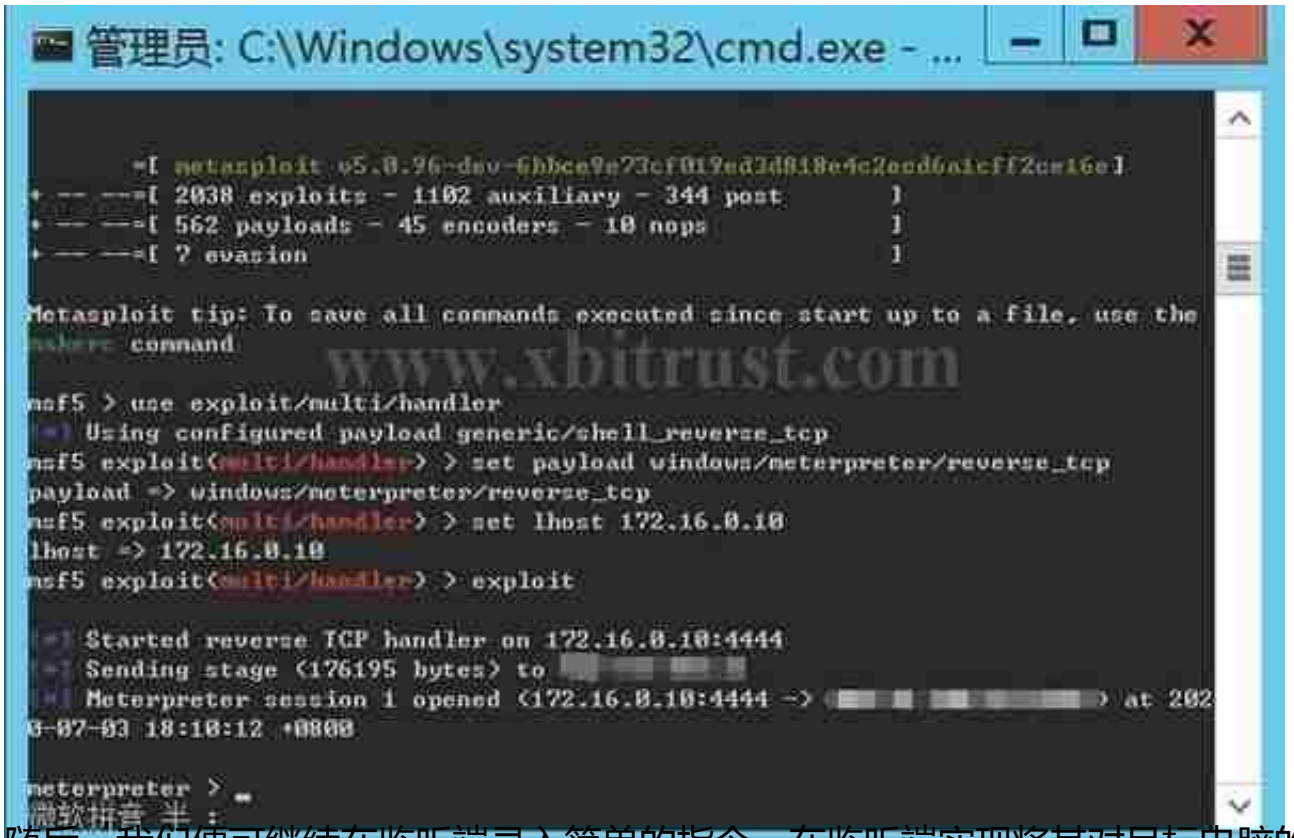
使用Fiddler可在一定程度上绕开网站对图像上传格式的限制。Fiddler是一个免费的Web调试代理工具，它记录计算机和因特网之间的所有HTTP(S)流量，可以检查通讯，设置断点和处理请求/响应。我们使用Fiddler设置断点，选择在请求之前截断请求，然后在网站中选择“伪装的头像”webshell.jpg上传。在拦截的Request信息中，Fiddler提供了方便的查看方式，其中包括Cookies、Raw、WebForms等。我们可将webshell.jpg改回webshell.html，然后继续响应请求。这样便成功上传了webshell.html文件。

这里的口令是为了防止其他黑客连接上我们的木马而设置的简单屏障，我们接着往下执行程序：



如上图所示，这些VBA代码在生成的new.vba文件之中。将这些代码复制到电子表格的Visual Basic编辑器中，并将宏名称取为“Auto_Open”，以便启动电子表格时自动运行。这样，此电子表格的宏只要被运行就将感染目标电脑。另外，还可以在此宏中添加一些其他代码以实现特定的任务，例如创建一个计划任务，每隔固定时间执行一次（非必要），并添加一个提示框。随后，我们将该电子表格进行传播。

在目标电脑端的测试中，若用户点击了此电子表格，该提示框便提示木马已成功运行或暗示用户已被感染（实际运用中不加此项）：



随后，我们便可继续在监听端录入简单的指令，在监听端实现将其对目标电脑的权限提升至系统权限、列出目标电脑的系统进程、截获音频、截屏、摄像头拍照和拍视频、记录键盘击键过程、开启远程桌面等功能。

四、针对Web服务器的DDoS攻击

DDoS攻击似乎与直接盗取比特币的关系不大，但其在数字货币领域会偶尔出现，故值得进行简要的阐述。2020年3月13日，BitMEX交易所就分别在北京时间10:16和20:56遭受了两次DDoS攻击。

（一）针对Web服务器的DDoS攻击简介[10]- [11]

DDoS攻击是指攻击者采用分布式攻击平台对一个或多个制定目标进行拒绝服务攻击，致使受到攻击的Web服务器或者网络无可用资源提供服务。

黑客们为了建立僵尸网络通常使用网络木马和网络蠕虫两种方法，网络木马通过恶意捆绑或程序漏洞等进行扩散，网络蠕虫通过系统漏洞、欺诈等方式传播。当计算机感染僵尸程序后，便在主控端和被感染计算机之间建立一个可一对多控制的网络——僵尸网络，僵尸网络的拥有者便可远程控制网络内的所有主机对目标服务器或目标主机发动应用层DDoS攻击。

为了达到既定的攻击伤害，僵尸网络建成之后，攻击者需对攻击目标进行探测，确定目标开放的服务和站点，即决定使用何种攻击流量。对于Web服务器的DDoS攻击往往需要探测更多信息数据，例如，需要探测Web服务器上哪些网页包含大内存的图片、哪些网页包含数据库动态查询功能。这些网页被攻击者所利用，会对Web服务器造成巨大威胁，通过不断地请求这些网页中资源消耗较大的节点，无形中增加了Web服务器资源消耗的速度，提高了攻击效率。DDoS 攻击开始时，僵尸主机将按照攻击者规划的攻击程序运行，向受害目标发送大量具有攻击行为的请求，因攻击行为皆为模仿正常用户访问行为所设计的，这造成目标服务器难以区分合法请求与非法请求，最终达到受害目标无可用服务资源提供服务的目的。

按照BitMEX交易所的博客所述，其在今年3月13日受到了两次相同的DDoS攻击，僵尸网络通过一个精心设计的聊天室功能查询使得该平台不堪重负。

据称，聊天室有七种语言，每种语言的简单频道ID为1到7，首先是英语，最后两个是西班牙语和法语。BitMEX相应的接口允许按频道ID来查询最后的100行。考虑到表的大小（大约5000万行），执行反向顺序扫描，然后进行筛选实际上会更快。查询优化程序对所有语言执行反向顺序扫描，直到最终找到要返回的100行。就西班牙语而言，很久没人聊天了，以至于扫描了849748行才能找到足够符合条件的行数。这种昂贵的顺序扫描快速地分配和释放大量内存，溢出到磁盘上，并通过系统调用迅速使得系统不堪重负。在攻击发生时，数据库只花了0.6%的时间处理请求，其余99.4%的时间用于IO等待，这便导致所有查询都非常慢。

虽然与用户相关的数据（电子邮件、活动、聊天室、登录事件等）与交易数据（仓位、交易、保证金等）是分开的，但是聊天室与用户有关，访问令牌和API密钥也是如此。这意味着这种资源消耗引发了位于交易引擎前面的身份验证和访问控制层的严重问题。交易引擎运行正常，市场数据、存款和提现也没有中断，但在这段时间内，请求几乎不可能到达引擎，导致服务质量严重下降。

这对于已经登录网站的用户，会发现攻击前原本因行情大幅波动而波涛汹涌的盘口，瞬间成为了平静的湖面，偶尔有小鱼跳动引发的涟漪，而当用户退出后就再也无法登录成功。

没有一个系统能够抵御DDoS的干扰，而有许多技术可以用来减少或消除影响。BitMEX称其已经解决了潜在的问题，并一直在昼夜不停地引入额外的检测和响应层，他们也将进行其他努力，以提高负载下的自动化扩展性和进一步隔离关键系统。BitMEX强调，作为上述持续监察和缓解措施的一部分，其安全团队正在审查系统中历史最悠久且因此最脆弱的部分，以简化、解耦、提高性能和隔离系统。同时，其团队正在开发关于宕机、市场暂停、市场恢复和通信的面向公众的协议，在将来其服务出现任何中断的时候，为其用户提供更大的透明度。

（二）DDoS攻击实践

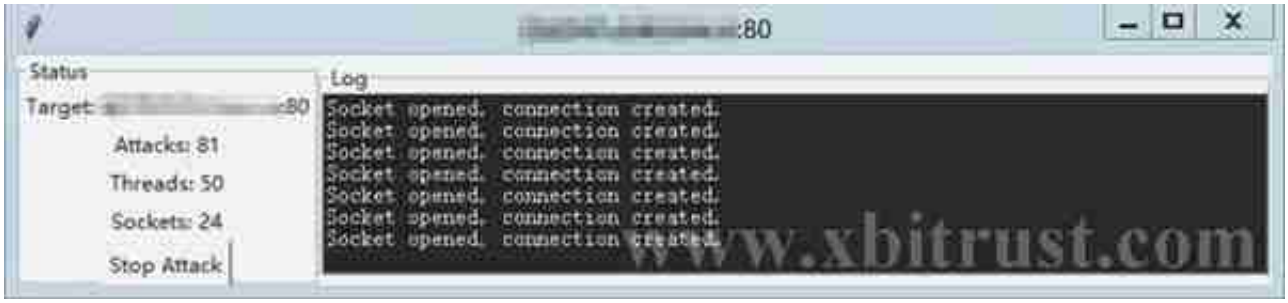
由于我们用于攻击的主机数量较少，严格地讲，我们下面进行的攻击实践应属于DoS攻击（拒绝服务攻击），只有当大量的主机参与攻击时才能称其为DDoS攻击（分布式拒绝服务攻击）。

通过编写程序，我们使用一些主机不断发送大量的数据包到某台自有服务器，希望造成该服务器资源耗尽，以至于宕机崩溃。不过由于发动攻击的主机数量较少，不易达成目标。此类攻击的程序示例在网络上比较多，这里就不再进行更详细的阐述和展示了。

我们也可以使用相关工具来开展攻击——下载pyloris模块来进行DoS中的Slowloris攻击。

在Slowloris攻击中，即使只使用一台PC也有可能使Web服务器陷入瘫痪。分析攻击原因时，通常使用Web服务器的日志，由于头文件分析结束时才记录日志，所以Slowloris攻击不会在日志文件中留下痕迹，这样就很难对其进行探测。正常的HTTP头以/r/n/r/n结束，Web服务器通过查找/r/n/r/n判断HTTP头结束，然后进行分析，处理服务请求。Slowloris攻击使用的HTTP头只以/r/n结尾，所以Web服务器认为HTTP头尚未结束，就无法对HTTP头进行分析，从而继续保持连接。当服务器连接数达到最大值时便无法继续处理新的请求，继而拒绝对外提供服务[12]。

从官网下载的pyloris模块的版本号是3.2，适用于Python
2。我们将其源码进行修改，使其能在Python
3中运行，然后在运行界面中填入要攻击的某自有测试网站的地址和端口：



五、结语

为了阐明盗取比特币的一些黑客技术，上文对网站渗透、木马、宏病毒和DDoS攻击进行了相关的浅显的介绍。尽管其中的DDoS攻击与直接盗取比特币的关系不大，但鉴于其重要程度以及对数字货币交易所的巨大影响，本文对其也做了简要的介绍。同时，我们还编写了较为简单的程序并利用一些工具对自有网站和主机进行了

攻击实践。这在一定程度上有助于普通用户对黑客基础技术的了解，促使人们积极地做好数字货币资产安全的防护工作。

由于篇幅所限，对于以上黑客技术和其他部分技术的综合运用以及相关的安全防护措施，我们将在今后的文章中进行详细的讨论。

参考文献

[1]吴松泽. 基于Web安全的渗透测试技术研究. 哈尔滨师范大学硕士学位论文, 2015. 9-11

[2] 蒲石. Web安全渗透测试研究. 西安电子科技大学硕士学位论文, 2010. 2-17

[3] 钱伟. 网站评估渗透系统的研究与实现. 复旦大学硕士学位论文, 2011. 6-7

[4] 贺瑞强. 木马的攻击及新型的木马检测技术的研究.
西安建筑科技大学硕士学位论文, 2009. 3-18

[5] 谢宗仁. 木马原理分析与实现. 山东大学硕士学位论文, 2009. 16-19

[6] 朱腾绩. 64位Windows木马关键技术研究与实现. 西安理工大学硕士学位论文, 2015. 2

[7]刘成光. 基于木马的网络攻击技术研究. 西北工业大学硕士学位论文,2004. 14

[8] 王津梁. Office漏洞挖掘与分析技术研究. 重庆理工大学硕士学位论文, 2017. 8-9

[9] 宏病毒原理及实现. 百度文库. https://wenku.baidu.com/view/c4f763dfa200a6c30c22590102020740bf1ecd32.html?fr=search

[10] 任皓. 针对WEB服务器的DDoS攻击与防御技术研究.
河北科技大学硕士学位论文, 2019. 9-10

[11] Arthur Hayes. 我们对于3月13日所遭受的DDoS攻击的回应. BitMEX Blog.https://blog.bitmex.com/zh_cn-how-we-are-responding-to-last-weeks-ddos-attacks/

[12] 赵诚文, 郑暎勋. Python黑客攻防入门. 武传海译. 北京: 人民邮电出版社, 2018.

182-183

本文链接：https://www.8btc.com/media/621090

转载请注明文章出处