CobaltStrike二次开发环境初探

_{原创}六号刃部 酒仙桥六号部队 2020-12-09原文

> 这是 **酒仙桥六号部队** 的第 124 篇文章。 全文共计2938个字,预计阅读时长9分钟。

在我们使用cobaltstrike的过程中,会涉及到二次开发,从而使其功能上更加的健壮,不至于碰到杀软就软了的地步,本文从cobalt strike的快速反编译到二次开发环境的准备作为二次开发cobalts trike的起步。

IntelliJ

IDEA自带了一个反编译java的工具,有时候我们需要对cobaltst rike 的 整 个 jar 包 进 行 反 编 译 , 使 用 这 个 IntelliJ IDEA双击之类的反编译时要是对整个源码层面进行搜索并不是很方 便,可使用其自带的反编译工具,可以做到批量的整个反编译。

- CobaltStrike反编译

这 里 先 在 Intellij IDEA 安 装 目 录 找 到 javadecompiler.jar 拷贝到一个准备好的目录,并且新建两个文件, 一个 cs_bin 里面放未反编译的 cobaltstrike 再建一个 cs_src文 件,这个是空文件,是为了之后放反编译后的 cobaltstrike

/Applications/IntelliJ IDEA.app/Contents/plugins/javadecompiler/lib/java-decompiler.jar //找到decompiler文件

cp java-

decompiler.jar /Users/name/Desktop/wen/学习资料/java/cstips001/

//拷贝到准备好的目录

ĥ.		升级 了解更多
Cstips001 (È ►	cs_bin cs_src java-decompiler.jar	cobaltstrike.jar

在java-decompiler中找到decompiler的路径,提取出来如下:

满.											
messages	O F	ietbrains	A 1	iava 📃	A 1	decompiler	code	0.	AssertProssor.class	0	BaseDecompiler.class
META-INF	>						IdeaDecompiler.class	0	ClassesPrssor.class	0	ConsoleDpiler.class
gro 📄	0						IdeaDeconion.class	0	ClassesPrr\$1.class	0	PrintStreagger.class
search	• •						IdeaDecoping.class	0	ClassesProde.class	0	
							IdeaDecopt\$1.class	0	ClassesPrtion.class	0	
							IdeaDecod\$1.class	0	ClassesPrnner.class	0	
							IdeaDecod\$2.class	0	ClassRefessor.class	0	
							IdeaDecovider.class	0	ClassWriter.class	0	
							IdeaDecoer\$1.class	0	ClassWriter\$1.class	0	
							IdeaDecos\$1.class	0	ClassWritType.class	0	
							IdeaDecoaver.class	0	collectors	0.	
							IdeaDecondle.class	0	decompiler	C) >	
							IdeaDecoleKt.class	0	Decompilntext.class	0	
							IdeaLogger.class	0	EnumProcessor.class	0	
							IdeaLoggption.class	0	extern	0.	
							IdeaLoggings.class	0	Fernflower.class	0	
							main	< ⊂ ►	Initializeressor.class	0	
							modules	0+	rels	0.	
							ShowDecction.class	0			
							struct	0.			
							util	0.			

org/jetbrains/java/decompiler/main/decompiler/

把路径提取出来后,把反斜杠全部替换成.随之再其后加上console Decompilers,如下就是提供反编译的这个类。

• •	📄 test.txt –	- 已编辑	
Q~/			🚳 < ゝ 完成 🗹 替換
			6 替换 全部
org.jetbrains.java.deo	compiler.main.decompiler.Co	onsoleDecompiler	
	-		

org.jetbrains.java.decompiler.main.decompiler.ConsoleDecompile

 因为
 MANIFEST.MF
 中 没有 main

 class属性,没有指定主类,因此不能直接使用 java

 jar,如果想要执行 java 包中具体的类,要使用 java

 cp输入如下命令:

java -cp java-decompiler.jar

org.jetbrains.java.decompiler.main.decompiler.ConsoleDecompiler

执行的时候会有提示。

cs_bin cs_src JeMacBook-Pro -/Deskto Jisaae: java -jar fernflower jar F-con	java-decompiler java-decompiler.jar p/wen/⊕5]∰14/java/cstips001 java -cp java-decompil tiono=cvalue>1* [<source/> 1+ <destination></destination>			
xample: java -jar fernflower.jar -dg Macsook-Pro	s=true c:\my\source\ c:\my,jor d:\decompiled\ dwende=dde=statovd(sstips:dime			
iL	你	加	Ŀ	-
dgs=true,	后跟需要反编译的		ike和反编译之后	要把cob
altstrike	e放入的目录,就	是我们最开始	建立的cs_src这	个是存放
反编译后的	cobaltstrike,	,运行这条命。	令即可对整个jar	包开始反
编译。				

ava -cp java-decompiler.jar
org.jetbrains.java.decompiler.main.decompiler.ConsoleDecompiler
-dgs=true cs_bin/cobaltstrike.jar cs_src/



反编译后,会自动打包成jar包,右键解压后打开可以看到都是.ja va了,使用这个方法会非常方便,就不需要第三方工具,这个反编译 出来的就可以直接放入 IntelliJ IDEA中,可直接实现代码搜索,相关的交叉引用。

Þ 🔚	aggressor	689.8 KB
▼ 💼	beacon	294.4 KB
	BeaconC2.java	35.1 KB
	BeaconCharsets.java	1.8 KB
	BeaconCommands.java	3.0 KB
	BeaconConstants.java	3.0 KB
	BeaconData.java	3.7 KB
	BeaconDNS.java	8.2 KB
	BeaconDownloads.java	5.0 KB
	BeaconElevators.java	1.4 KB
	BeaconErrors.java	5.9 KB
	BeaconExploits.java	1.4 KB
	BeaconHTTP.java	4.2 KB
	BeaconParts.java	1.6 KB
	BeaconPayload.java	14.5 KB
	BeaconPipes.java	1.6 KB
	BeaconPivot.java	1.4 KB
	BeaconRemoteExecMethods.java	1.5 KB
	BeaconRemoteExploits.java	1.8 KB
	BeaconSetup.java	4.1 KB
	BeaconSocks.java	6.9 KB
	BeaconTabCompletion.java	16.2 KB
_ ▶	c2setup	5.1 KB
	CheckinListener.java	686 B
	CommandBuilder.java	3.0 KB
▶	dns 📃	10.5 KB
▶	elevators	1.5 KB
	EncodedCommandBuilder.java	1.5 KB

二 Cobalt	Strike二次开发环	境				
打 开	IntelliJ	IDEA	选	择	Create	New
Project-	一直选择Next。					
Java Enterprise JBoss Spring Java FX Android IntelliJ Platform Plugin Spring Initializr Quarkus MicroProfile Maven Gradle Gradle Grave Application Forge Kotlin JavaScript Flash Empty Project	Project SDK: 18 java version "1.8.0.221" Additional Libraries and Frameworks: JBoss Arquillian JUnit Arquillian TestNG JBoss Drools Arquillian TestNG JBoss Drools Arquillian TestNG JBoss Drools Arquillian TestNG Sping Contexts and Dependency Inject Thymeleaf E Conditional Comments support Java 8 Time API compatibility Spring 3 integration Spring 4 integration Spring Security 3 integration Spring Security 4 integration Spring 2 integration Tiles 2 integration 	New Project				Ţ
? Cancel						Previous Next

这里选择路径跟起个名。

• • •		New Project	
Project name:	MycustomCS		
Project location:	/Users_	学习资料/java/cstips/project	•••

创建好后需要先建立两个文件夹,右击选择 New Directory建立一个decompiled_src文件夹,之后再建立一个li b文件夹。

micitematicarians Scratches and Consols	
Search Everywhere Double 17	
Go to File 0.80	
Recent Files ¥E	
Navigation Bar ¥ ↑	
New Directory	
decampled_sec	

把在CSTips001中反编译好的CobaltStrike复制到decompiled_ src中,然后把它解压出来,可看到一个完整的反编译后的目录。



随后把原始的未编译的CobaltStrike放到刚刚新建的lib中去。



接下来需要对这个项目进行设置,点击File中的Project Structure在Modules对Dependencies进行设置。

IntelliJ IDEA	File Edit View Navig	gate Code	Analyze	Refactor	Build	Run	Tools	VCS	Window	Help	예 🔹 😌 👘 🖓 🖓 🕹 👘 🖓	p" 🖷
project [Mycu idea idea is is src Mycustom(lill) External Libra	New Copen Open Recent Close Project File Project Structure File Properties Save All Calead All from Disk.	+ ;% ;% 2% Y%7									MyoustomCS	
Scratches and	Invalidate Caches / Rest Manage IDE Settings New Projects Settings	tart		•••			- 6				Project Structure	
	Export Print Add to Favorites))		Project Set Project Modules	ttings	Ng N	- Aycustor	nCS		Name: N Sources	rces Paths Dependencies	
	Power Save Mode			Libraries Facets Artifacts Platform S SDKs Global Li Problems	ettings braries s					Module SI Export	ule SDK: Rg Project SDK 1.8	
选	择			1	ib				F	ŧ	的 cobalt	

strike.jar,确认是Compile之后勾选一下,然后选择Apply。





至此依赖关系设置完了,现在进入Artifacts-->JAR-->From

			Project Structure
$\leftarrow \rightarrow$			
Project Settings	Add		
Project	💠 JAR		Empty
Modules	JavaFx Application	۲	From modules with dependencies
Libraries	Solution: Exploded		
Facets	Web Application: Explored		
Artifacts	http://www.communication Application: Exploded		

modules with dependencies

这里需要一个填写一个Main Class



目前我们还不知道这个 Main Class 该填什么,可以点在lib中的 META-INF 里双击 MANIFEST.MF,我们可以看到 Main Class,复制aggressor.Aggressor



再	次	打	开	Artifacts>JAR>From modules	with
dep	penc	denc	ies	在	Main
Cla	ass	と 填り	lag	gressor.Aggressor选择OK,这里就设置完)	成了。



接下来在decompiled_src目录中找到已经反编译完的aggressor 主类,右击选择Refactor --Copy File

<code>project</code> $ angle$ decompiled_src $ angle$ aggressor $ angle$	💰 Aggressor.java			
👩 🗖 Project 👻 🕀 🛨	\$ −			
 project [MycustomCS] ~/De idea decompiled_src aggressor bridges bridges browsers biologs headless ui viz windows 				
Aggressor.java	New			
AggressorClient.java	X Cut	жх		
DataManager.java	Copy D Paste	* %∨		
👌 DataUtils.java	Find Usages	Έ Γ7		
d GlobalDataManager.	Analyze			
💰 MultiFrame.java	Refactor	×	Rename	
SelectOnChange.jav	Add to Favorites		Rename File	
SyncMonitor.java	Reformat Code	\C#L	Move File Copy File	F6 F5
WindowCleanup.jav	Optimize Imports Delete	^∖_0 ∞	Safe Delete	жø
beacon	Build Module 'MycustomCS'		Generify	
 C2profile Cloudstrike 	Baycal in Finder		Add Right-to-Left (RTL	.) Support
	Reveal in Finder			
	Сору			
Copy file /Users	Copy /project/decompiled_s	src/aggre	ssor/Aggressor.jav	a
Copy file /Users	Copy /project/decompiled_s ava	src/aggre	ssor/Aggressor.jav	a
Copy file /Users New name: Aggressor.j To directory:	Copy 'projec t/decompiled_s ava /学习资料/java/cstips/pro	src/aggres	ssor/Aggressor.jav	a r 🔻
Copy file /Users New name: Aggressor.j To directory: Use ^Space f	Copy 'project/decompiled_s ava /学习资料/java/cstips/pro	src/aggre)ject/decor	ssor/Aggressor.jav npiled_src/aggresso	a r 🕶
Copy file /Users New name: Aggressor.j To directory: Use ^Space f ? V Open in editor	Copy 'projec t/decompiled_s ava /学习资料/java/cstips/pro	src/aggre	ssor/Aggressor.jav mpiled_src/aggresso Cancel	a r 💌 Refactor

在

ТΟ

directory点击添加,选择之前创建的src在其中添加一个aggres sor名字要一致,最后点击Refactor

	•	Сору				
Favorites Recents Applications Desktop Oownloads iCloud Cloud Cloud Drive Desktop Documents Locations Comments Co	 iCloud storage decompile lib Mycustom src Name of negative aggressor k Pro	ge is full. d_src	META-INF		Upgrade) (Learn More)
Media New Folder					Cancel	Open
		Сору	/			
Copy file /Use	Aggressor java	/project/decom	piled_src/ag	gressor/Aggr	essor.java	
i ton namo.	Aggreeourijara					
To directory:	/Users	/学习资	¥料/java/cstip	s/project/src/a	ggressor	•
	Use ^Space for path (completion				
? 🗹 Open i	n editor			Can	cel Re	factor

这样aggressor就自动的被拷贝到src目录里去了,这里可以看一

下,如图。



测试一下,修改文件,保存。

project / src / aggressor / 🌚 Aggressor / 💭 mair	
🔲 Project 👻 😌 🛨 🖊 🗢	G Aggressorjava 🛛
🔻 📑 project [MycustomCS] ~/Desktop/wen,	1 package aggressor;
🕨 🖿 .idea	
decompiled_src	
🕨 🖿 lib	
	12 > public class Aggressor {
🔻 🖿 aggressor	<pre>13 public static final String VERSION = "4.0 (20191205) " + (License.isTrial() ? "Trial" : "Licensed");</pre>
😅 Aggressor	14 public static MultiFrame frame = null;
META-INF	
🛃 MycustomCS.iml	16 public static MultiFrame getFrame() { return frame; }
Illi External Libraries	
I.ibrary/Java/JavaVirtualMach	28 b public static void main(String[] var@) {
Scratches and Consoles	21 TotionPana chawMacangaDining(harantComponent will message: "hello from wikeso");
	22 Baccanfonding Jackall Sconnel (an Jackall Sci Jacka
	22 refer contage.installesoupe constant(or c, a (verse), 23 Bancesonafia (installesonactante (in (in (installes)))
	Parservoni igi instaluces upe constant (0, , a (uber 1),
	<pre>24 Parsercontg.installescapeLonstant(0: '0', 's: '\user'); 07</pre>
	25 (new usesynthetica()).setup();
	26 Requirements.oneckbul()
	<pre>27 License.checkLicense6UI(new Authorization());</pre>
	28 frame = new MultiFrame();
	29 (new ConnectDialog(frame)), show();

到这里我们的整个准备工作就完成了,之后就是我们要修改哪个文件,就可以在完整的源码中找到那个文件,然后右键Refactor然后 Copy

File到这个目录然后进行修改,修改完成之后就可以选Build-->Build Artifacts -->Build进行编译。



当提示Build completed successfully in 4 s 227 ms (a

minute

ago)的时候,会生成一个out文件夹,其中可看我们的编译好的MycustomCS.jar



在每次调试运行的时候,不需要切换到命令行环境,可以直接选择_Run中的Profile设置参数。



选择十号,在JAR Applic添加一个配置文件。



在 Path to JAR中选择out文件中我们修改并编译好的jar包,选择好后点击Ap

•••		Andr	oid Profiler - CustomRu	in			
+ - 🖻 🗡 🔺	< > 💷 🖹	i My	customCS_jar				re as project file 🔅
▼ II JAR Applicat	Favorites Recents A Applications Desktop Downloads icloud icloud Drive Desktop Documents Locations Remote Disc Remote Disc Network Media	iCloud storage is full. sustomCS_jar	MycustomCS.jar		Upgrac J Mycusto Java JAR fil Tags Created J	te) Learn More) mCS.jar le - 27 MB Vdd Tags Forday 3:11 PM	
	New Folder	 → Before launch ● Warning: JAR file '/' 	doesn't exist		Canc	el Open	
?						Cancel	pply Profile

最后在Run中选择Run CustoomRUn即可看到消息窗。



点击确定,发现弹出提示,没关系,继续点击确定。

Java -XX:+AggressiveHeap option not set. Use the Cobalt Strike launcher. Don't click the .jar file!

确定

我们把-XX:+AggressiveHeap复制下来。



再放到Run的Profile这里就直接选择之前创建的CustomRun填入V M options 最后选择Apply



	Edit configuration settings	
Name: CustomRun	Allow parallel run Store as proje	ct file 🔍
Configuration Code Cov	verage Logs	
Path to JAR:	:tips/project/out/artifacts/MycustomCS_jar/MycustomCS	.jar 🚞
VM options:	-XX:+AggressiveHeap	
Program arguments:		
Working directory:	Isers//学习资料/java/cstips/project	
Environment variables:		
Redirect input from:		
JRE:	Default (<no jre=""> - module not specified)</no>	
Search sources using mod	dule's classpath: <pre><pre><pre><pre><pre><pre><pre>dule's classpath:</pre></pre></pre></pre></pre></pre></pre>	
• Refore launch		
	There are no tasks to run before launch	
+ - / * *		
I Error: Android Profiler: 1	there are no runners for JAR Application: CustomRun	
?	Cancel Apply	Profile

再次Run运行,继续复制-XX:+UseParallelGC

/Lbraw/Jaw/Jews/stalkablas/jdil.1.8.221.jd/Context/News/sib/jaw -GX:+AgpresiveNap -Dflt.essadorpUTF-8 -jar /Inccs/ //FIRM/inv/stlas/sciet/act/actifacts/ProstanCL_isc [-] Jaw / OX:-UsersetiteEpstion not set. Use the Cobalt Strike lawscher. Don't click the .jar file! Process finished with exit code 8

继续在添加到VM options中,记得要用空格隔开。

	Edit configuration settings						
Name: CustomRun	Allow parallel run Store as proje	ct file 🔅					
Configuration Code Co	overage Logs						
Path to JAR:	:tips/project/out/artifacts/MycustomCS_jar/MycustomCS.jar 🔚						
VM options:	-XX:+AggressiveHeap -XX:+UseParallelGC	+ 2					
Program arguments:							
Working directory:	Isers,						
Environment variables:							
Redirect input from:							
JRE:	Default (<no jre=""> - module not specified)</no>						
Search sources using mo	odule's classpath: <whole project=""></whole>						
✓ Before launch							
+ - / + -							
• Error: Android Profiler:	: there are no runners for JAR Application: CustomRun						
(2)	Cancel Apply	Profile					

再次运行,提示auth文件找不到。

))					
					Connect			
			New Profile	This is the connect to Host: Port: User: Password:	connect dialog. You should use it to a Cobalt Strike (Aggressor) team server. 50050 neo •••••••••••••••••••••••••••••••••••			
			· · · · · · · · · · · · · · · · · · ·					
	CustomRun ×							
1	/Library/Java/JavaVirtualMag	chines/	jdk1.8.0_221.jdk/C	ontents/Hom	e/bin/java -XX:+AggressiveHeap -XX:+	UseParallelGC -Dfile.encoding=UTF-		
1	[-] Trapped java.io.FileNot!	FoundEx	ception during rea	dFile: /Use	rs//学习资料/java/	stips/project/out/artifacts/Myrus	tomCS_jar/cobaltstrike.	auth [main]: /Users/
Ľ	java.io.FileNotFoundException			p/wen/学习资料	料/java/cstips/project/out/artifacts,	/MycustomCS_jar,cobaltstrike.auth		
E								
÷								
1								
1								

这里把初始的 cobaltstrike.auth 文件复制到 MycustomCS.jar 同目录下。

iCloud 储存空间已满。				升级	了解更多
iCloud 储存空间已满。 artifacts production		MycustomCS_jar (1		升级 cobaltstrike.auth MycustomCS.jar	了解更多 ① ①
11	11		11		11

最后运行,到这里我们需要进行二次开发的环境就搭建好了,接下来 就可以根据我们的需要通过关键字在源码中定位到具体的功能实现 的代码,从而进行修改,或作一些功能上的增强。

31	}			Connect	
32		New Profile	This is the connect to	connect dialog. You should use it to a Cobalt Strike (Aggressor) team serve	er.
			Host:		
			Port:	50050	
			User:	neo	
			Password:	******	
				Connect Help	
CustomRun ×					
/Library/Java/JavaVirtualMachi	ines/jdk1.8.0_22	1.jdk/Contents/Hom	e/bin/java	-XX:+AggressiveHeap -XX:+UsePara	llelGC -Dfile.encoding=UTF-8 -j

三 总结

 文
 使
 用
 IntelliJ

 IDEA自带的java反编译工具,对cobaltstrike进行了快速的反编
 译,并展示了修改后的效果,权当抛砖引玉,具体的插件开发各位

 师傅可以结合具体场景进行编写。

参考资料

红队学院CSTips





长按二维码关注 酒仙桥六号部队

精选留言

用户设置不下载评论