FA2022 Week 03 Rev/Pwn Setup

Minh and Pete



Announcements

- Fall CTF 2022
 - This Saturday!!! 12 6PM
 - CIF 3039



ctf.sigpwny.com sigpwny{i_love_nsa_software} NOW AND THEN, I ANNOUNCE "I KNOW YOU'RE LISTENING" TO EMPTY ROOMS.

IF I'M WRONG, NO ONE KNOWS. AND IF I'M RIGHT, MAYBE I JUST FREAKED THE HELL OUT OF SOME SECRET ORGANIZATION.



Outline

- **Goal:** Get everyone set up with Ghidra, Python, and pwntools in preparation for Thursday, Reverse Engineering I
- Installing Java Developer Kit
 - Windows
 - Mac Intel
 - Mac M1
 - Linux
- Installing Ghidra
- Installing Python, pwntools, GDB



What is Ghidra?

- Ghidra is a reverse engineering toolkit developed by the NSA and made open source
- Allows you to disassemble applications essentially turn an unreadable application into readable code



			Godebrowsen: test:/Grack		
File Edit Analysis Naviga	ation Search Se	lect Tools Window Help F S V B・ 油油 Юつ ノ間り	s = c, ≛ O H ♦ = s	8.9	
Program Trees	Listing: Crack			a	C Decompile FIIN 05045648 . (Cord)
ringiant trees (1) (1) (1)	Country, Chart		- 101 No. 4 35		
Crack Sonool Tree Sonool Tree		// represent 2.1: // Lostable segm // fail BMB300 essure DF = 000 (Defacti) essure DF = 000 (Def	nt [0x8040000 - 0x844831 -00040113 7Fh c. "ELF" c. 1b c. 1b c. 2h c. 3h c. 1b c. 2h c. 2h c. 1b c. 2h	ldent_regi ldent_regi	<pre>2 int fUL_00048648(int argt,char **argv) 4 5 long lVar1; 6 9 // Var1 = price(PTMACE_TRACHE.a,l,0); 9 // var1 = of a debuguer 1'); 10 obort(); 11 obort(); 12 // var1 = of a debuguer 1'); 13 if (argc.[= 2) { 14 puts(*You nut give a password for use this program 1*); 15 // WOUNDG Subroutine does not return */ 16 abort(); 17 // var1 = of a password for use this program 1*); 18 if (argc.[= 2) { 19 puts(*You nut give a password for use this program 1*); 19 puts(*Debugsad(argv[1]); 20 } 21 } </pre>
	Console - Scriptin	ng l			A //
Filter:					
3				08	3048000



JDK on Windows



Installing Java Developer Kit

Install JDK 11 (not JRE!) from Oracle

https://www.oracle.com/java/technologies/javase/jdk11-archivedownloads.html

or Google "oracle java se 11"

ORACLE Products Indust	tries Resources Customers Partners Developers Events	Q O View Accounts
Linux ARM 64 Compressed Archive	157.21 MB	[➡] jdk-11.0.16_linux-aarch64_bin.tar.gz
Linux x64 Debian Package	138.42 MB	🛃 jdk-11.0.16_linux-x64_bin.deb
Linux x64 RPM Package	144.60 MB	🛃 jdk-11.0.16_linux-x64_bin.rpm
Linux x64 Compressed Archive	161.08 MB	ظِّ jdk-11.0.16_linux-x64_bin.tar.gz
macOS Arm 64 Compressed Archive	153.35 MB	°₩ jdk-11.0.16_macos-aarch64_bin.tar.gz
macOS Arm 64 DMG Installer	152.83 MB	°, jdk-11.0.16_macos-aarch64_bin.dmg
macOS x64 Compressed Archive	155.47 MB	°₩ jdk-11.0.16_macos-x64_bin.tar.gz
macOS x64 DMG Installer	154.95 MB	°₩ jdk-11.0.16_macos-x64_bin.dmg
Solaris SPARC Compressed Archive	184.75 MB	'₩ jdk-11.0.16_solaris-sparcv9_bin.tar.gz
Windows x64 Installer	140.55 MB	°₩ jdk-11.0.16_windows-x64_bin.exe
Windows x64 Compressed Archive	158.30 MB	idk-11.0.16_windows-x64_bin.zip

JDK on Intel/M1 Mac



Installing Java Developer Kit

Go to https://brew.sh and run the setup command

If it is already installed, make sure to update with `brew update`

Install openjdk java11 or newer: `brew install java11`



Linking Java

Caveats
For the system Java wrappers to find this JDK, symlink it with
sudo ln -sfn /opt/homebrew/opt/openjdk@11/libexec/openjdk.jdk /Library/Java/JavaVirtualMachines/openjdk-11.jdk

openjdk@11 is keg-only, which means it was not symlinked into /opt/homebrew, because this is an alternate version of another formula.

If you need to have openjdk@11 first in your PATH, run: echo 'export PATH="/opt/homebrew/opt/openjdk@11/bin:\$PATH"' >> ~/.zshrc

Link your Java JDK

THESE COMMANDS SHOULD BE COPIED FROM END OF BREW OUTPUT

sudo ln -sfn /opt/homebrew/opt/openjdk@11/libexec/openjdk.jdk
/Library/Java/JavaVirtualMachines/openjdk-11.jdk

Run 'java -version' to check that openjdk 11 (or newer) is found

~/ java -version
 openjdk version "11.0.16.1" 2022-08-12
 OpenJDK Runtime Environment Homebrew (build 11.0.16.1+0)
 OpenJDK 64-Bit Server VM Homebrew (build 11.0.16.1+0, mixed mode)
 ~/ 4

If it isn't found, add jdk11 to your path

echo 'export PATH="/opt/homebrew/opt/openjdk@11/bin:\$PATH"' > ~/.zshrc
&& source ~/.zshrc



JDK on Linux

Note that we recommend installing JDK and Ghidra on Windows instead of WSL



Installing JDK

sudo apt update
sudo apt install openjdk-11-jdk

 Newer JDKs are OK That's it!



Downloading Ghidra

https://github.com/NationalSecurityAgency/ghidra/releases

or Google "github ghidra release"

Download the public archive in assets for the latest release (ghidra_X.X.X_PUBLIC_XXXXXXX.zip, not Source code.zip)

Ghidra 10.1.5 Latest		
 What's New Change History Installation Guide SHA-256: 17db4ba7d411d11b00d1638f163ab5d61ef38712cd68e462eb8c8556 	ec5cfb5ed	
▼ Assets ₃		
	328 MB	Jul 26, 2022
Source code (zip)		Jul 26, 2022
Source code (tar.gz)		Jul 26, 2022
③ ▲ 62 ④ 7 ⊯ 31 ● 26 2 12 00 7 89 people reacted		



Running Ghidra

Windows: Double click ghidraRun.bat

Mac/Linux:

Open Terminal, navigate to the directory where Ghidra is downloaded using something like `cd ~/Downloads/ghidra_XX` Make ghidraRun executable: `chmod +x ./ghidraRun` Launch Ghidra: `./ghidraRun`



Python and Pwntools



What is pwntools?

pwntools is a CTF framework and exploit development library. Intended to make exploit writing as simple as possible.

```
>>> sh = process('/bin/sh')
>>> sh.sendline(b'sleep 3; echo hello world;')
>>> sh.recvline(timeout=1)
b''
>>> sh.recvline(timeout=5)
b'hello world\n'
>>> sh.close()
```



Installing Python

Mac:

brew install python
python3 -m ensurepip

Windows (WSL)/Linux:

sudo apt update && sudo apt install python3
python3-pip

We recommend Windows users use Python/pwntools in WSL rather than native Windows

Installing Pwntools

pip3 install pwntools
OR
pip install pwntools

M1 Setup before pwntools

```
$ git clone
https://github.com/unicorn-e
ngine/unicorn.git
$ brew install cmake
$ brew install qemu
$ cd unicorn/bindings/python
$ python setup.py install
```

If you get "command not found" you may need to reboot for Python/pip to be added to PATH



Installing GDB

Non M1 Mac: brew install gdb M1 Mac: x86 emulator required, stick around Windows (WSL)/Linux: sudo apt install gdb

We recommend Windows users use Python/pwntools in WSL rather than native Windows

Next Meetings

If you are on a M1 Mac please stick around!

2022-09-22 - This Thursday

- Reverse Engineering I
- Use the tools we installed today to reverse engineer apps!

2022-09-24 - This Saturday

- Fall CTF 2022
- fallctf.sigpwny.com
- 2022-09-25 Next Sunday
- No meeting



x86 VM on M1 Mac

For debugging and running x86 applications



Warning

- M1 macs run a ARM-based processor
- We want to run a x86-based linux VM
- Virtualization
 - Fast
 - Docker, VirtualBox
 - Target architecture must be same as hardware architecture
- Emulation
 - Slow
 - qemu, UTM
 - Hardware architecture can be anything



Install UTM

• <u>mac.getutm.app</u>

Download an AMD64/x86 VM (e.g. Ubuntu 22.04 LTS)

• <u>ubuntu.com/download/desktop</u>

Ubuntu Server 22.04 recommended

• Desktop GUI will be extremely slow



- Open UTM
- "Start from Scratch"

•••	+ UTM	
	You can download an existing VM configuration for popular operating systems from the UTM gallery or start from scratch.	
	Go To Gallery	
	Start from Scratch	
		This virtual machine has been deleted.

- Set the architecture
- Set the memory limit to 4 or more GB
- Turn on Force
 Multicore with 0
 Cores

	(i) Information	System	QEMU	Drives	D isplay	iiiii Input	() Network	(」)) Sound	Sharing		
	Hardware										
rchitecture	x86_64										\bigcirc
System	Standard PC (Q3	5 + ICH9,	2009) (al	lias of pc	-q35-6.1)	(q35)					\bigcirc
Memory										4096	MB
	Show Advanced	d Settings									
	Tweaks										
	🗹 UEFI Boot										
	CPU										
	Default										\bigcirc
	CPU Cores										
										0 C	ores
	V Force Multicore)									
	Set to 0 to use maximum supported CPUs. Force multicore might result in incorrect emulation.										

- Add the ISO as a USB device
- Create a second IDE Disk > 20GB
- Leave all other settings (Display, Input, etc.) default



Desktop

- Follow normal Ubuntu installation
- Install the minimal installation and don't download updates

Server

• Accept all defaults

	~~ ~ ~ ~
Sep 18 05:44	. ()
Install	×
Updates and other software	•
 What apps would you like to install to start with? Normal installation Web browser, utilities, office software, games, and media players. Minimal installation Web browser and basic utilities. Other options 	
 Download updates while installing Ubuntu This saves time after installation. Install third-party software for graphics and Wi-Fi hardware and additional media formats This software is subject to license terms included with its documentation. Some is proprietary. 	

Quit

Back

Continue

- After the installer finishes, remove the USB drive from the "Drives" section
- Restart UTM



retep@retep-Standard-PC-Q35-ICH9-2009:~\$ uname -a
Linux retep-Standard-PC-Q35-ICH9-2009 5.15.0-47-generic #51-Ubuntu SMP Thu Aug 1
1 07:51:15 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux

