逆向工程入门: IDAwindows本地动态调试, linux远程动态调 试及虚拟机配置

原创

June_giy ● 于 2021-02-11 09:50:29 发布 ● 595 ☆ 收藏 2 分类专栏: 网络安全 文章标签: ubuntu linux vmware 安全 版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/weixin_50549897/article/details/113772269</u> 版权



4 篇文章 1 订阅 订阅专栏

本人水平有限,有不当之处欢迎指出

文章目录

- 一、虚拟机配置
- 二, IDA动态调试

1.windows本地调试

2.linux远程调试

本人其它文章链接

一、虚拟机配置

VMware虚拟机是主流的虚拟机之一。我主要讲VMware Workstation Pro虚拟机的创建。首先从官网上下载VMware Workstation Pro。

官网链接

从各种渠道获取密钥后可以开始使用。 接着从ubuntu官网下载64位或32位的linux操作系统镜像 ubuntu官网 (tips:从网上其它渠道下载可能速度会更快)

打开VMware,再文件里选择新建虚拟机





在选择安装镜像光盘文件里选择你要安装

的操作系统的镜像文件

• [

L	新建虚拟机向导	\times
	安装客户机操作系统 虚拟机如同物理机,需要操作系统。您将如何安装客户机操作系统?	
	安装来源:	
	◯ 安装程序光盘(D):	
	● 安装程序光盘映像文件(iso)(M):	
	D:\ubuntu-16.04-desktop-i386.iso	
	已检测到 Ubuntu 16.04。 该操作系统将使用简易安装。(这是什么?)	
	○ 稍后安装操作系统(S)。	
	创建的虚拟机将包含一个空白硬盘。	
	帮助 < 上一步(B)。// 下一步(N) >// 取消()	897
下一步命名设置密码	等等	
	新建虚拟机同导	XI

新建虚拟机向导	\times
指定磁盘容量 磁盘大小为多少?	
虚拟机的硬盘作为一个或多个文件存储在主机的物理磁盘中。这些文件最初很小随着您向虚拟机中添加应用程序、文件和数据而逐渐变大。	`,
最大磁盘大小 (GB)(S): 20.0 🖕	
针对 Ubuntu 的建议大小: 20 GB	



₩ 🔿

American English

二,IDA动态调试

1.windows本地调试

尽量使用IDA7.5进行调试,以下版本可能有bug

首先设置断点



		00000604 main	:5 (400604)									
0utp	ut window											0 8 ×
选择	local windows debu	ugger后按F9升	干始调试									
File E	dit Jump Search View Debugger	Lumina Options Windo	ws Help									
: 📂 🖬	← ▼ → ▼ ª * * * * 4 4	20 🕱 🗟 🖆 🗗 📌 🔍	🖬 🗙 🗄 🕨 🖬 Local Vindovs 🤉	lebugger 🔻 🗞 🕻	2 : 🗰 🗗 🖤							
Lib	rary function <mark> Regular function </mark>	Instruction 📃 Data 📃 Un	explored External symbol 📕 Lu	mina function							4	
	Debug View		Structures	(3	E	nums	×				
	IDA View-EIP	×	Pseudocode-A	×				👿 General :	registers			- 8
1 2 3 4 5	<pre>intcdecl main(int a { int Str; // [esp+1Ch _BYTE v5[96]; // [es</pre>	rgc, const char] [ebp-68h] BYR p+20h] [ebp-64h	**argv, const char EF] BYREF	**envp)				 EAX 0000000 EBX 002EA00 ECX 00401AF EDX 0000000 ESI 0040120 	01 4 00 4 00 4 00 4 00 4 00 4			▲ ID 0 VIP 0 VIF 0 AC 0 VM 0 RF 0
06	main();							🔝 Modules				- <i>8</i>
 7 8 9 10 	<pre>Str = 0; memset(v5, 0, sizeof printf("Please give scanf("%100s", &Str) Create Mar();</pre>	(v5)); me the flag:"); ;						Path C:\User	s\June\De dowe\SveV	sktop\逆向迷宫 //OW64\dtramr	题\2020maze.exe	>
1 1 2	if (stplop();	hop *)85+p)	EQ && chock((chop *	85+n))				🔄 Threads				- 8
12	puts(")pC0pgpatu1a	tional Youn fl4	g is platt ")	(astr))				Decimal	Hex	State	Name	
14	else		g 13 (1g)(C.),					31400	7AA8	Running	2020maze.ex	e
• 15	puts("\nSorrerrerr	rrv~")·						🔄 11680	2DA0	Running	773B7F60	
- 13		119-73						00156	AERC	Dunning	77387660	
	00000993 _main:1 (401593)							~ (
O Hex	View-1	C1 EQ Q4 QQ C2 QD 4E	检幼梅检			_ = * ×	OCTEFAC COM		alabal db			0.6
004015 004015 004015 004015 004015 004015	00 00<	61 60 89 62 85 43 65 08 84 07 40 78 81 88 45 E8 83 E8 91 88 45 E8 83 E8 91 80 81 C4 94 00 00 94 60 81 C4 94 00 00 94 60 83 C4 80 E8 E0 5 30 8D 54 24 20 88 00	\$1. the\$1. the				0061FEA0 0044 0061FEA4 0006 0061FEA8 753F 0061FEAC 0071 0061FEB0 0061 0061FEB4 7546	FGFB9 msvcrt LOC9C debug0 LFEBC Stack[DGFF5 msvcrt	:.dll:msvci 34:00710C9 00007AA8] :.dll:msvci	rtonexit+109 9C :0061FEBC rtunlock+15		
000009	90 00401390: _check+117					`	UNKNOWN UUG1FE	AU: Stack[00	00/AA8]:00	GIFEAU (Synchro	onized with ESP)	
0utp 751700	ut window MM0: loaded C:\Windows\SvsWDW64\1	MM32.DLL										- 8
74AE6	A0: thread has started (tid=2220 : loading symbols for 'C:\Users\	08) June\Desktop\逆向迷宫题	A\2020maze.exe'									

PDB5KS: loading symbols for 'C:\Users\June\Desktop\沙问还昌型\2020maze.exe'... PDB: using PDBIDA provider Could not find PDB file ''. Please check _MT_SYMEDU_PATH PDB: Failed to get PDB file details from 'C:\Users\June\Desktop\逆向迷宫题\2020maze.exe' Perform

按F8向下一条一条执行,在debugger—debugger windows—locals窗口里可以查看变量的值和相应的地址。

File Edi	i Jump Searci	n view	Del	bugger Lumina Options w	indows H	lei	p												
📂 🖬	(m) ▼ (m) ▼ (m) ∂ ⁿ ₁₁ δ	6 6 B		Quick debug view	Ctrl+2		🕨 🔲 💶 Local Windows	debugger 🔹	'e 🛃 i 🗊 🕈 🕈	ĸ									
Libra	ry function I	Regular Debug Vie		Debugger windows Breakpoints Watches) 		General registers Segment registers				Enun:	1111 1.S					A V		•
	IDA Viev-EIP	×		Tracing	•	5	MMX registers		ls (HEXRAYS)	×				👿 General r	egisters			- <i>6</i>	×
Name argc > argv > envp Str > v5		Value 1 0x6E1 0x6E1 0x363 {0,0,0,		Continue process Attach to process Process options Pause process Terminate process Detach from process Refresh memory Take memory snapshot	F9 Ctrl+F2		KMM registers XMM registers XMM registers Debugger window Thread list Module list Locals Stack view Stack trace CLUE	Ctrl+Alt+C Ctrl+Alt+S						EAX 0000000 EBX 00307000 ECX 25734D9 EDX 00406060 ESI 004012D I Nodules Path I C:\Users	1 4 0 4 TIB[0 5 4 3 4 .rdat. 0 4 _main Vune\Des	0004A9C]:00307000 a:a100s+5 CRTStartup Constitute: constitute: ktop\逆向迷宫题\2	020maze.exe	ID 0 VIP 0 VIF 0 AC 0 VM 0 RF 0	
			P C	Step into	F7 E8	5	Watch view							<	OWELSIJEM	(OW64)dtrampo d		>	× .
			ф П	Run until return Run to cursor	Ctrl+F7 F4									🔄 Threads				- 8	×
			*c 2	Switch to source Use source-level debugging Open source file Debugger options										Decimal 19100 24356 28776	Hex 4A9C 5F24 7068	State Ready Ready Poody	Name 2020maze.exe 773B7F60 773B7E60	>	^ ~
🖸 Hex Vi	ew-1			Switch debugger		F					×		Stack view						×
00401550 00401560 00401570 00401580 00401580 00401580	00 00 00 00 EC 01 D0 05 00 00 00 00 39 45 F4 7C 5F 5D C3 55 00 00 C7 44	EB 34 8 20 80 4 EB 14 8 84 B8 6 89 E5 5 24 1C 6	3B 4 40 6 33 4 91 6 57 8 90 6	15 F0 C1 E0 04 89 C2 88 00 0F B6 00 84 C0 74 07 15 F4 01 88 55 88 58 88 10 00 00 81 C4 94 00 00 13 E4 F0 83 C4 80 E8 E 10 00 00 8D 54 24 20 88 10	45 38 30 9E魔· 30 9E魔· 35 _]肬· 30荄·	.€@ @ (個 (個	i, 鸽,'擇. 嬪. , 翰. t , 嬪. 缓 ₩森. 譜. 朣. 桀 峊. \$				Â		061FEA0 0040 061FEA4 0061 061FEA8 753F 061FEAC 006E 061FEB0 0061 061FEB4 7540	6063 .rdata FEBC Stack 6FB9 msvcrt 0C9C debug FEBC Stack 6FF5 msvcrt 00: Stack100	:a100s 00004A9C] .dll:msvc 35:006E0C 00004A9C] .dll:msvc	:0061FEBC rt_onexit+109 90 :0061FEBC rt_unlock+15 061FEA0 (Synchroni	zed with ESP)		~
Output	window											1						- <i>-</i>	~
75170000 74AE6FA0): loaded C:\k): thread has	lindows\ started	Sys (t	WOW64\IMM32.DLL id=20220)		_						_				https://	blog.csdn.net/weixir	_505498	^

2.linux远程调试

首先打开IDA的dbgsrv复制里面的linux_server(对应32位)或linux_server64(对应64位),黏贴到对应的linux虚拟机。并且将需 要调试的文件也复制过去。

我以一个32位的ELF文件为例。

打开虚拟机的终端,输入ifconfig查看ip(inet后面)





接下来cd 到linux_server的目录(我这里是Desktop)输入./linux_server启动,可以看到正在监听23946端口

Ter	minal	1	TL 🖇 🕬)) 12:06 AM 🕄
	Deijing	S S June@ubuntu: ~/Desktop june@ubuntu:-S ipconfig	
	linux_server	No command 'ipconfig' found, did you mean: command 'inconfig' from package 'iwriteless-tools' (main) command 'ikconfig' from package 'wireless-tools' (main) ipconfig: command not found ipconfig: command not found incaubuntu:-\$ ifconfig ens33 Link encap:Ethernet HWaddr 00:0c:29:e2:24:33 Inet addr: Dest Ethernet HWaddr 00:0c:29:e2:24:33 Nach	
	LibreOffice Impress	Inet addr: fe80::dda:1287:4065:cf4a/64 Scope:Link UP BROADCAST RUNNING MULIICAST MTU:1500 Metric:1 RX packets:77 errors:0 dropped:0 overruns:0 frame:0 TX packets:77 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:12631 (12.6 KB) TX bytes:8461 (8.4 KB) Interrupt:19 Base address:0x2000	
		<pre>lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr:::1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:213 errors:0 dropped:0 overruns:0 frame:0 TX packets:213 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1 RX bytes:16399 (16.3 KB) TX bytes:16399 (16.3 KB)</pre>	
		june@ubuntu:-/S cd Desktop june@ubuntu:-/DesktopS linux_server Linux_server: command not found june@ubuntu:-/DesktopS ./linux_server IDA Linux 32-bit remote debug Server(ST) v7.5.26. Hex-Rays (c) 2004-2020 Listening on 0.0.0.0:23946 2021-02-09 00:03:49 [1] Accepting connection from the termination of termina	
		https://blog.csdr	n.net/weixin_50549897

如果出现以下情况表明没有权限



需要输入以下命令给权限

然后在IDA的调试选remote linux debugger,按F9.





如果IDA显示无法连上虚拟机则需要关闭防火墙或重置虚拟网卡。

关闭防火墙: 先输入以下,然后输入三次原密码

sudo passwd

再输入

su root

接着输入以下命令关闭防火墙

ufw disable

若还不行则重置虚拟网卡,见以下这篇文章 https://www.jianshu.com/p/d70622414101

本人其它文章链接

逆向迷宫题总结(以四道题目为例)

BUUCTF reverse: [GXYCTF2019]luck_guy,findit,简单注册器题解

封神台靶场尤里的复仇I第一第二第五第六第七章解题思路(持续更新)

ctfhub:网鼎杯第一场2018 reverse-beijing题解