

PSP0201

Week 5

Writeup

Group Name: ikun no 1

Members

ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 17: Reverse Engineering ReverseELFneering

Tool used: Kali-Linux

Solution/walkthrough:

Question 1

TryHackMe | 25 Days of C x

https://tryhackme.com/room/learnycyberin25days

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title	IP Address	Expires
aoccmnr2	10.10.206.129	32m 37s

Perform arithmetic operations on registers and data

Transfer control to other parts of the program Since the architecture is x86-64, the registers are 64 bit and Intel has a list of 16 registers:

Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	d	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

When dealing with memory manipulation using registers, there are other cases to be considered:

Find the answer in THM.

Question 2

TryHackMe | 25 Days of C x

https://tryhackme.com/room/learnycyberin25days

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title	IP Address	Expires
aoccmnr1	10.10.4.210	32m 37s

analysing binaries. It can be used to disassemble binaries(trans user to step through the execution and view the state of the p

Luckily for us, everything we need has been provided to you via

1. Press the "Deploy" button on the top-right of this task
2. Wait for the IP address of the target Instance to display
3. Log into your Instance using the following information:

IP Address: 10.10.4.210

Username: elfmceager

Password: adventofcyber

Let's proceed to run through how Radare2 works exactly. Although you shouldn't do this if the program is unknown, it is safe for us to execute to see what should be happening like so:

```
File Actions Edit View Help
(1211103206@kali) ~
$ ssh elfmceager@10.10.4.210
The authenticity of host '10.10.4.210 (10.10.4.210)' can't be established.
ED25519 key fingerprint is SHA256:Y18Ef38JQ7HNTMf6qew50LnmIqEXXSzLqgX82k/Rsg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.4.210' (ED25519) to the list of known hosts.
elfmceager@10.10.4.210's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-128-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Tue Jul 12 03:45:57 UTC 2022

System load: 0.0          Processes:           91
Usage of /:  39.4% of 11.75GB   Users logged in:    0
Memory usage: 8%           IP address for ens5: 10.10.4.210
Swap usage:  0%
```

Use ssh and the password and username that had given to login the account.

The screenshot shows a web browser window displaying the TryHackMe room page for 'learnrcyberin25days'. The page includes a table with columns 'Title', 'IP Address', and 'Expires'. The first row shows 'aocmnre1' with IP '10.10.4.210' and an expiration time of '10.18.11.248'. Below the table, there are instructions for the task, including a list of steps: 1. Press the "Deploy" button on the top-right of this task. 2. Wait for the IP address of the target Instance to display. 3. Log into your Instance using the following information: IP Address: 10.10.4.210, Username: elfmceager, Password: adventofcyber. A terminal window is overlaid on the page, showing the command 'ls' and the output 'challenge1 file1'. The terminal also shows the command 'r2 -d ./challenge1' and the output 'Process with PID 1447 started...'. The terminal further shows the command 'afl -i ./challenge1' and the output 'Using 0x400000'. The terminal also shows the command 'afl -i ./challenge1' and the output 'Warning: Cannot initialize dynamic strings'. The terminal also shows the command 'afl -i ./challenge1' and the output 'asm.bits 64'. The terminal also shows the command 'afl -i ./challenge1' and the output '[0x00400a30] aa'. The terminal also shows the command 'afl -i ./challenge1' and the output '[WARNING : block size exceeding max block size at 0x006ba220]'. The terminal also shows the command 'afl -i ./challenge1' and the output '[+] Try changing it with e anal.bb.maxsize'. The terminal also shows the command 'afl -i ./challenge1' and the output 'WARNING : block size exceeding max block size at 0x006bc860'. The terminal also shows the command 'afl -i ./challenge1' and the output '[+] Try changing it with e anal.bb.maxsize'. The terminal also shows the command 'afl -i ./challenge1' and the output '[x] Analyze all flags starting with sym. and entry0 (aa)'. The terminal also shows the command 'afl -i ./challenge1' and the output '[0x00400a30] afl | grep main'. The terminal also shows the command 'afl -i ./challenge1' and the output '0x00400b4d 1 35 sym.main'. The terminal also shows the command 'afl -i ./challenge1' and the output '0x00400de0 10 1007 -> 219 sym.__libc_start_main'. The terminal also shows the command 'afl -i ./challenge1' and the output '0x00403840 39 661 -> 629 sym._nl_find_domain'. The terminal also shows the command 'afl -i ./challenge1' and the output '0x00403ae0 308 5366 -> 5301 sym._nl_load_domain'.

Is and open the file. Then, use aa command to analyse it.

Question 3

The screenshot shows a web browser window displaying the TryHackMe room page for 'learnrcyberin25days'. The page includes a table with columns 'Title', 'IP Address', and 'Expires'. The first row shows 'aocmnre1' with IP '10.10.4.210' and an expiration time of '10.18.11.248'. Below the table, there are instructions for the task, including a list of steps: 1. Press the "Deploy" button on the top-right of this task. 2. Wait for the IP address of the target Instance to display. 3. Log into your Instance using the following information: IP Address: 10.10.4.210, Username: elfmceager, Password: adventofcyber. A terminal window is overlaid on the page, showing the command 'ls' and the output 'challenge1 file1'. The terminal also shows the command 'r2 -d ./challenge1' and the output 'Process with PID 1447 started...'. The terminal further shows the command 'afl -i ./challenge1' and the output 'Using 0x400000'. The terminal also shows the command 'afl -i ./challenge1' and the output 'Warning: Cannot initialize dynamic strings'. The terminal also shows the command 'afl -i ./challenge1' and the output 'asm.bits 64'. The terminal also shows the command 'afl -i ./challenge1' and the output '[0x00400a30] aa'. The terminal also shows the command 'afl -i ./challenge1' and the output '[WARNING : block size exceeding max block size at 0x006ba220]'. The terminal also shows the command 'afl -i ./challenge1' and the output '[+] Try changing it with e anal.bb.maxsize'. The terminal also shows the command 'afl -i ./challenge1' and the output 'WARNING : block size exceeding max block size at 0x006bc860'. The terminal also shows the command 'afl -i ./challenge1' and the output '[+] Try changing it with e anal.bb.maxsize'. The terminal also shows the command 'afl -i ./challenge1' and the output '[x] Analyze all flags starting with sym. and entry0 (aa)'. The terminal also shows the command 'afl -i ./challenge1' and the output '[0x00400a30] afl | grep main'. The terminal also shows the command 'afl -i ./challenge1' and the output '0x00400b4d 1 35 sym.main'. The terminal also shows the command 'afl -i ./challenge1' and the output '0x00400de0 10 1007 -> 219 sym.__libc_start_main'. The terminal also shows the command 'afl -i ./challenge1' and the output '0x00403840 39 661 -> 629 sym._nl_find_domain'. The terminal also shows the command 'afl -i ./challenge1' and the output '0x00403ae0 308 5366 -> 5301 sym._nl_load_domain'.

Use afl to set a breakpoint.

Question 4

