به نام خدا

سیستم های نهفته بی درنگ

تمرین شماره 4

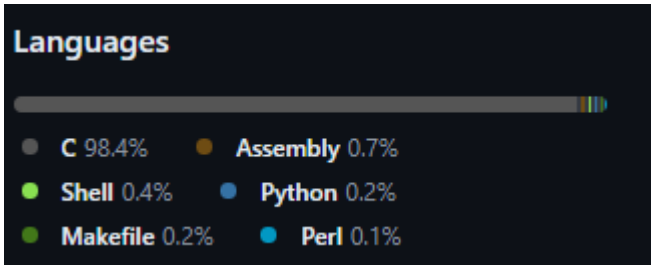
استاد: دکتر غلامپور

دانشجویان: حسین انجیدنی 400100746

تیر ماه 1403

سوال اول

الف)



تصویر توزیع زبان ها به کار رفته در کرنل لینوکس

سیستم عامل لینوکس عمدتاً به زبان C نوشته شده است، اما برخی از قسمت‌های آن به زبان اسمبلی نوشته شده‌اند. این بخش‌ها شامل قسمت‌هایی هستند که نیاز به دسترسی مستقیم به سخت‌افزار دارند یا باید با کارایی بسیار بالایی اجرا شوند. در زیر به تفصیل به این بخش‌ها و دلایل استفاده از زبان اسمبلی در هر کدام پرداخته شده است:

1.راه‌اندازی(Bootstrap)

- **بخش اسمبلی :**کدهای اولیه راه‌اندازی (bootloader) و کدهای ابتدایی کرنل که سیستم را از حالت بوت به حالت عملیاتی می‌برند.
- **علت استفاده :**در این مرحله، سیستم هنوز به طور کامل راه‌اندازی نشده و محیط اجرایی لازم برای اجرای کدهای C فراهم نیست. بنابراین، از زبان اسمبلی استفاده می‌شود که مستقیماً با سخت‌افزار در ارتباط است و می‌تواند وظایف اولیه مثل تنظیمات اولیه پردازنده و حافظه را انجام دهد.

2.مدیریت وقفه‌ها(Interrupt Handling)

- **بخش اسمبلی :**کدهای مدیریت وقفه‌ها و استثناها.
- **علت استفاده :**این کدها باید با سرعت و کارایی بالا اجرا شوند و مستقیماً با سخت‌افزار پردازنده در ارتباط باشند. زبان اسمبلی به دلیل سرعت بالا و توانایی دسترسی مستقیم به رجیسترها و منابع پردازنده، برای این منظور مناسب است.

3.مدیریت حالت هسته و کاربر(Kernel and User Mode Switching)

- **بخش اسمبلی :**کدهای سوئیچ کردن بین حالت هسته و حالت کاربر.
- **علت استفاده :**این کدها باید با کارایی بسیار بالا و به صورت بهینه اجرا شوند. همچنین، نیاز به دسترسی مستقیم به رجیسترها و تنظیمات پردازنده دارند که با زبان اسمبلی به راحتی امکان‌پذیر است.

4.روال‌های خاص پردازنده(Processor-Specific Routines)

- **بخش اسمبلی :**توابع و روال‌هایی که به صورت خاص برای پردازنده‌های مختلف نوشته شده‌اند.

- **علت استفاده :**این توابع برای بهره‌برداری کامل از قابلیت‌ها و ویژگی‌های خاص هر پردازنده نوشته شده‌اند و نیاز به دسترسی مستقیم به رجیسترها و تنظیمات خاص دارند.

5.بهینه‌سازی‌های سطح پایین**(Low-Level Optimizations)**

- **بخش اسمبلی :**بخش‌هایی از کد که نیاز به بهینه‌سازی‌های بسیار خاص و دقیق دارند.
- **علت استفاده :**زبان اسمبلی به برنامه‌نویس اجازه می‌دهد تا کنترل کامل بر روی کد و سخت‌افزار داشته باشد و از این طریق می‌تواند بهینه‌سازی‌های دقیقی را اعمال کند که با زبان C امکان‌پذیر نیست.

نتیجه‌گیری

استفاده از زبان اسمبلی در کرنل لینوکس به دلایل کارایی، دسترسی مستقیم به سخت‌افزار، و نیاز به اجرای بهینه و سریع در برخی بخش‌های خاص ضروری است. هر چند که بیشتر کرنل به زبان C نوشته شده است تا خوانایی و نگه‌داری کد آسان‌تر شود، اما در بخش‌هایی که نیاز به دسترسی مستقیم به سخت‌افزار و کارایی بالا وجود دارد، از زبان اسمبلی استفاده می‌شود.

ب)

آسیب‌پذیری‌های بحرانی اخیر در هسته لینوکس

در اینجا به پنج آسیب‌پذیری بحرانی اخیر در هسته لینوکس اشاره می‌کنیم:

1. آسیب‌پذیری اجرای کد از راه دور**(CVE-2022-47939)**

- **شرح :**این آسیب‌پذیری استفاده پس از آزادسازی (use-after-free) در ماژول سرور فایل SMB به نام ksmbdدر هسته لینوکس می‌تواند به مهاجم غیرمجاز از راه دور اجازه دهد که کد دلخواه را اجرا کند. مشکل در تابع DISCONNECT_TREE_2SMBاست که قبل از انجام عملیات بر روی شیء، وجود آن را بررسی نمی‌کند.
- نمره) 10.0 **:CVSSv3** بحرانی(
- **زمان تشخیص و رفع :**این باگ در تاریخ 17 اوت 2022 در نسخه 5.15.61 هسته لینوکس رفع شد. رفع این باگ شامل تصحیح مدیریت حافظه در تابع DISCONNECT_TREE_2SMBبود. کاربران سیستم‌های آسیب‌پذیر باید پچ‌های موجود را اعمال کنند.
- منبع[Tenable](#) :

2. آسیب‌پذیری**Dirty Pipe**

- **شرح :**این آسیب‌پذیری که توسط مکس کلرمن کشف شد، بر نسخه‌های 5.8 و بعد از هسته لینوکس تأثیر می‌گذارد. این باگ به مهاجم اجازه می‌دهد تا داده‌های فایل‌های فقط خواندنی را بازنویسی کند و منجر به افزایش دسترسی شود.
- **زمان تشخیص و رفع :**این نقص در به‌روزرسانی‌های اخیر هسته لینوکس رفع شده است. مشکل با تنظیم فلگ‌های بافر پایپ در کد منبع هسته لینوکس رفع شد.
- **منبع TechRadar :**

3. **تقسیم بر صفر در درایور نمایش AMD**

- **شرح :**یک باگ در درایور نمایش AMD مربوط به تنظیم پیکربندی فشرده‌سازی جریانی (DSC) می‌تواند منجر به خطای تقسیم بر صفر شود وقتی پارامتر height_slice برابر صفر تنظیم شود. این باگ می‌تواند کرنل را خراب کند و نیاز به راه‌اندازی مجدد سیستم دارد.
- **زمان تشخیص و رفع :**این باگ در آخرین به‌روزرسانی‌های هسته لینوکس رفع شده است. رفع این باگ شامل تصحیح نحوه مدیریت پارامترهای پیکربندی DSC در درایور نمایش AMD بود.
- **منبع The Register :**

4. **افزایش دسترسی در نسخه‌های کرنل 5.14 تا 6.6.14**

- **شرح :**یک آسیب‌پذیری جدید کشف شده به یک مهاجم محلی اجازه می‌دهد تا به دسترسی ریشه (root) در سیستم آسیب‌پذیر دست یابد با استفاده از یک نقص در مدیریت برخی از فراخوانی‌های سیستمی.
- **زمان تشخیص و رفع :**این آسیب‌پذیری در به‌روزرسانی‌های اخیر هسته لینوکس رفع شده است. راه‌حل شامل تصحیح مدیریت فراخوانی‌های سیستمی آسیب‌پذیر بود.
- **منبع The Register :**

5. **بایپس احراز هویت در ماژول SFTP انتقال MOVEit**

- **شرح :**این آسیب‌پذیری بر ماژول SFTP انتقال MOVEit تأثیر می‌گذارد و می‌تواند تحت شرایط خاصی منجر به بایپس احراز هویت شود.
- **زمان تشخیص و رفع :**این آسیب‌پذیری به تازگی کشف و رفع شده است. رفع این مشکل شامل تصحیح احراز هویت در ماژول SFTPبود.
- **منبع The Register :**

توصیه می‌شود که کاربران سیستم‌های آسیب‌پذیر تمامی به‌روزرسانی‌ها و پچ‌های امنیتی موجود را اعمال کنند تا از سوءاستفاده‌های احتمالی جلوگیری شود.

ج) تمام فرایند ها توسط دستورات لینوکس و برنامه rclone انجام شده که در تصویر زیر قابل مشاهده میباشد.

فایل در این لینک قابل دسترسی میباشد (لازم به ذکر است که این لینک نیز توسط rclone ساخته شده.)

```
hosein@hoseinonthego:~/Enb/HW04$ sudo pat install rclone

[sudo] password for hosein:
1209
Sorry, try again.
[sudo] password for hosein:
sudo: pat: command not found
hosein@hoseinonthego:~/Enb/HW04$ sudo apt install rclone
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1 linux-headers-6.5.0-26-generic linux-hwe-6.5-headers-6.5.0-26 linux-image-6.5.0-26-generic linux-modules-6.5.0-26-generic linux-modules-extra-6.5.0-26-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  rclone
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 11.7 MB of archives.
After this operation, 42.6 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 rclone amd64 1.53.3-4ubuntu1.22.04.2 [11.7 MB]
Fetched 11.7 MB in 7s (1,621 kB/s)
Selecting previously unselected package rclone.
(Reading database ... 268579 files and directories currently installed.)
Preparing to unpack .../rclone_1.53.3-4ubuntu1.22.04.2_amd64.deb ...
Unpacking rclone (1.53.3-4ubuntu1.22.04.2) ...
Setting up rclone (1.53.3-4ubuntu1.22.04.2) ...
Processing triggers for man-db (2.10.2-1) ...
hosein@hoseinonthego:~/Enb/HW04$ rclone config
2024/06/27 16:28:24 NOTICE: Config file "/home/hosein/.config/rclone/rclone.conf" not found - using defaults
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> mydrive
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Provider (AWS, Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio, Tencent COS, etc)
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Box
   \ "box"
 7 / Cache a remote
   \ "cache"
 8 / Citrix Sharefile
   \ "sharefile"
 9 / Dropbox
   \ "dropbox"
10 / Encrypt/Decrypt a remote
   \ "crypt"
11 / FTP Connection
   \ "ftp"
12 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
13 / Google Drive
   \ "drive"
14 / Google Photos
   \ "google photos"
15 / Hubic
   \ "hubic"
16 / In memory object storage system.
   \ "memory"
17 / Jottacloud
   \ "jottacloud"
18 / Koofr
   \ "koofr"
19 / Local Disk
   \ "local"
20 / Mail.ru Cloud
   \ "mailru"
21 / Microsoft Azure Blob Storage
   \ "azureblob"
22 / Microsoft OneDrive
   \ "onedrive"
23 / OpenDrive
   \ "opendrive"
24 / OpenStack Swift (Rackspace Cloud Files, Memset Memstore, OVH)
   \ "swift"
25 / Pcloud
   \ "pcloud"
26 / Put.io
   \ "putio"
27 / SSH/SFTP Connection
   \ "sftp"
28 / Sugarsync
   \ "sugarsync"
29 / Transparently chunk/split large files
   \ "chunker"
30 / Union merges the contents of several upstream fs
   \ "union"
31 / Webdav
   \ "webdav"
32 / Yandex Disk
   \ "yandex"
33 / http Connection
   \ "http"
34 / premiumize.me
   \ "premiumizeme"
35 / seafile
   \ "seafile"
Storage> 13
** See help for drive backend at: https://rclone.org/drive/ **

Google Application Client Id
Setting your own is recommended.
See https://rclone.org/drive/#making-your-own-client-id for how to create your own.
If you leave this blank, it will use an internal key which is low performance.
Enter a string value. Press Enter for the default ("").
client_id>
```

```
client_id>
OAuth Client Secret
Leave blank normally.
Enter a string value. Press Enter for the default ("").
client_secret>
Scope that rclone should use when requesting access from drive.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value
 1 / Full access all files, excluding Application Data Folder.
   \ "drive"
 2 / Read-only access to file metadata and file contents.
   \ "drive.readonly"
   / Access to files created by rclone only.
 3 | These are visible in the drive website.
   | File authorization is revoked when the user deauthorizes the app.
   \ "drive.file"
   / Allows read and write access to the Application Data folder.
 4 | This is not visible in the drive website.
   \ "drive.appfolder"
   / Allows read-only access to file metadata but
 5 | does not allow any access to read or download file content.
   \ "drive.metadata.readonly"
scope> 1
ID of the root folder
Leave blank normally.

Fill in to access "Computers" folders (see docs), or for rclone to use
a non root folder as its starting point.

Enter a string value. Press Enter for the default ("").
root_folder_id>
Service Account Credentials JSON file path
Leave blank normally.
Needed only if you want use SA instead of interactive login.

Leading `~` will be expanded in the file name as will environment variables such as `${RCLONE_CONFIG_DIR}`.

Enter a string value. Press Enter for the default ("").
service_account_file>
Edit advanced config? (y/n)
y) Yes
n) No (default)
y/n> n
Remote config
Use auto config?
 * Say Y if not sure
 * Say N if you are working on a remote or headless machine
y) Yes (default)
n) No
y/n> y
If your browser doesn't open automatically go to the following link: http://127.0.0.1:53682/auth?state=oO-TMvWYpki1-4Qu3Hfq8g
Log in and authorize rclone for access
Waiting for code...
Got code
Configure this as a team drive?
y) Yes
n) No (default)
y/n> n
--------------------
[mydrive]
scope = drive
token = {"access_token":"ya29.a0AXooCguHrtQ70P7T1FCdfkEA_878z-w_UyR8g5aFjTIbWGlmFUG1t8nI0C4IE68Xn9NY7Wnx3aVGgL15SmcDERGBGAtKqLqYeExgS3LOM_B41SzGng4Cd7qu3AdJZAlfh42nuKNLOUQs1PeVv8OAiqymvokX6nKMilFZaCgYKAWgSARASFQHGX2Mi43JYPOTmzKPDVNKmGWzAHW0171","token_type":"Bearer","refresh_token":"1//09dXBKpyr-M2_CgYIARAAGAkSNwF-L9Ir5_eCus0leNNCW8bBJf2QJueDDkRYlY67C-UQoCagjYHgRXGyMprxM-XdrRtJZA6npzE","expiry":"2024-06-27T17:30:54.341688718+03:30"}
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d> y
Current remotes:

Name                 Type
====                 ====
mydrive              drive

e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
hosein@hoseinonthego:~/Emb/HW04$ cd Q1
hosein@hoseinonthego:~/Emb/HW04/Q1$ echo "" > EmbeddedGoogle.txt
hosein@hoseinonthego:~/Emb/HW04/Q1$ rclone copy EmbeddedGoogle.txt mydrive:
2024/06/27 16:34:54 Failed to create file system for "mydrive:": couldn't find root directory ID: Get "https://www.googleapis.com/drive/v3/files/root?alt=json&fields=id&prettyPrint=false&supportsAllDrives=true": net/http: TLS handshake timeout
hosein@hoseinonthego:~/Emb/HW04/Q1$ rclone copy EmbeddedGoogle.txt mydrive:
hosein@hoseinonthego:~/Emb/HW04/Q1$ rm EmbeddedGoogle.txt
hosein@hoseinonthego:~/Emb/HW04/Q1$ ls
gdrive.sh
hosein@hoseinonthego:~/Emb/HW04/Q1$ rclone copy mydrive:EmbeddedGoogle.txt .
hosein@hoseinonthego:~/Emb/HW04/Q1$ ls
EmbeddedGoogle.txt  gdrive.sh
hosein@hoseinonthego:~/Emb/HW04/Q1$ echo "$(date)" >> EmbeddedGoogle.txt
hosein@hoseinonthego:~/Emb/HW04/Q1$ echo "Hossein Anjidani" >> EmbeddedGoogle.txt
hosein@hoseinonthego:~/Emb/HW04/Q1$ echo "400100746" >> EmbeddedGoogle.txt
hosein@hoseinonthego:~/Emb/HW04/Q1$ echo "hoseinanjidani2@gmail.com" >> EmbeddedGoogle.txt
hosein@hoseinonthego:~/Emb/HW04/Q1$ echo "09331480365" >> EmbeddedGoogle.txt
hosein@hoseinonthego:~/Emb/HW04/Q1$ rclone copy EmbeddedGoogle.txt mydrive:
hosein@hoseinonthego:~/Emb/HW04/Q1$ rclone link mydrive:EmbeddedGoogle.txt
https://drive.google.com/open?id=1npO61wYZZ-lweXkq1Ewm_veq7tUQsNY8
hosein@hoseinonthego:~/Emb/HW04/Q1$ S
```

سوال دوم

خروجی های این سوال در یک فیلم ده دقیقه ای نمایش داده شده است.

در این سوال از libssh استفاده شده است و تمامی خروجی ها و مراحل کار با آن در فیلم آمده است.

فرایند اجرای cmake به شکل زیر است:

```
Cmake -DRH=”server adddress” -DUN=”username” -DPASS=”password” -DCPU=cpu_limit -DMEM=memory_limit
```

در فایل های SSH_Connection توابعی موجود است که به ssh متصل میشود و توسط تابع execute دستور مورد نظر ارسال میشود.

فایل CMAKE List:

در این فایل افزون بر معرفی فایل ها برای ساخت فایل make متغیر های موجود در دستور قبل تعریف شده است که جایگزین در فایل main.cpp میشود.

سوال سوم

الف)

این کد با استفاده از هدر های فایرفاکس نوشته شده است؛ همچنین خروجی های این کد به شرح زیر است که در تصویر صفحه بعد آمده است.

ب)

خروجی این بخش در فایل news.txt موجود است. که به شرح زیر است:

Scraped on 2024-06-29 15:13:47

عضویت استاد دانشگاه صنعتی شریف در هیئت تحریریه نشریه معتبر از انجمن شیمی آمریکا (ACS)

دانشگاه صنعتی شریف میزبان میهمانان جشن بزرگ غدیر

آغاز عملیات اجرایی ساخت استادسرای پونک دانشگاه صنعتی شریف

نصب نشان عالی دانش بر سینه استاد برجسته دانشگاه صنعتی شریف

آخرین احکام صادره

برگزاری مراسم دعای عرفه در مسجد دانشگاه

```
 EmbeddedGoogle.txt  'Screenshot from 2024-06-27 16-42-21.png'  'Screenshot from 2024-06-27 16-42-40.png'
hosein@hoseinonthego:~/Emb/HW04/Q1$ cd ..
hosein@hoseinonthego:~/Emb/HW04$ cd Q3
hosein@hoseinonthego:~/Emb/HW04/Q3$ ls
installnet2service.sh  intsallScrapperService.sh  net2.service  net2.sh  scrapper.service  webscrapping.py
hosein@hoseinonthego:~/Emb/HW04/Q3$ sh
installnet2service.sh      intsallScrapperService.sh  net2.sh
hosein@hoseinonthego:~/Emb/HW04/Q3$ sh net2.sh
Checking connection...
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6089  100  6089    0     0  13813      0 --:--:-- --:--:-- --:--:-- 13807
Connection checked you are not logged in ....
Trying to login ...
<html>
<head>
<title>mikrotik hotspot > redirect</title>
<meta http-equiv="refresh" content="2; url=http://net2.sharif.edu/status">
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="expires" content="-1">
<style type="text/css">
<!--
textarea,input,select {
        background-color: #FDFBFB;
        border: 1px #BBBBBB solid;
        padding: 2px;
        margin: 1px;
        font-size: 14px;
        color: #808080;
}

body{ color: #737373; font-size: 12px; font-family: verdana; }

a, a:link, a:visited, a:active { color: #AAAAAA; text-decoration: none; font-size: 12px; }
a:hover { border-bottom: 1px dotted #c1c1c1; color: #AAAAAA; }
img {border: none;}
td { font-size: 12px; color: #7A7A7A; }

-->
</style>
<script language="JavaScript">
<!--
    function startClock() {
                location.href = 'http://net2.sharif.edu/status';
    }
//-->
</script>
</head>
<body onLoad="startClock()">
<table width="100%" height="100%">
<tr>
        <td align="center" valign="middle">
        You are logged in
        <br><br>
        If nothing happens, click <a href="http://net2.sharif.edu/status">here</a></td>
</tr>
</table>
</body>
</html>
Checking connection...
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1159  100  1159    0     0   3711      0 --:--:-- --:--:-- --:--:--  3714
You have already logged in.
```

سوال چهارم:

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

^Chosein@hoseinonthego:/media/hosein/Local Disk/Uni/Sem 6/RES/HWs/HW04/Q4$ ./run_prime_sum.exp
spawn ./PrimeSum
Enter a positive integer: 25
25 = 2 + 23
do you want to continue?
yes
finishedReached end of file unexpectedly.
spawn ./PrimeSum
Enter a positive integer: 50
50 = 3 + 47
do you want to continue?
yes
50 = 7 + 43
do you want to continue?
yes
50 = 9 + 41
do you want to continue?
yes
50 = 13 + 37
do you want to continue?
yes
50 = 19 + 31
do you want to continue?
yes
finishedReached end of file unexpectedly.
spawn ./PrimeSum
Enter a positive integer: 100
100 = 3 + 97
do you want to continue?
yes
100 = 11 + 89
do you want to continue?
yes
100 = 17 + 83
do you want to continue?
yes
100 = 29 + 71
do you want to continue?
yes
100 = 41 + 59
do you want to continue?
yes
100 = 47 + 53
do you want to continue?
yes
finishedReached end of file unexpectedly.
hosein@hoseinonthego:/media/hosein/Local Disk/Uni/Sem 6/RES/HWs/HW04/Q4$
```

همچنین خروجی **GDB** در فایل دیباگ موجود است.