מעבדה 4:

מגיש 1: גיל אלגריסי 209286699

מגיש 2:רועי זולטי 31465302

Part 1:

1.1

```
gil_roy@gpu-03:~/0450112_Cyber_lab/Lab4/ASLRLab$ python3 check.py 1a
make: Nothing to be done for 'all'.
Checking part 1A...
100%|
You passed 1000 of 1000 runs (100.0%)
Success! Good job

Your score is 20 / 20
You scored 100.0% for this part!
gil_roy@gpu-03:~/0450112_Cyber_lab/Lab4/ASLRLab$
```

1.2

Another system call that could be used for egg hunting is **mincore**.

<u>Why mincore Works:</u>

The “mincore” system call determines whether pages in a specified memory range are resident in memory.

Like access, it will return an error (EFAULT) if the address is not valid or mapped.

1.3

```
gil_roy@gpu-03:~/0450112_Cyber_lab/Lab4/ASLRLab$ python3 check.py 1b
make: Nothing to be done for 'all'.
Checking part 1B...
100%|
You passed 999 of 1000 runs (99.9%)
Success! Good job

Your score is 40 / 40
You scored 100.0% for this part!
```

1.4

As an Intel engineer, the goal is to mitigate the side-channel vulnerability arising from timing differences between prefetching mapped and unmapped addresses.

<u>Enforce Access Controls for prefetch</u>

- Introduce access checks to the prefetch instruction to validate whether the address is accessible to the current process.
- If the address is not accessible, the prefetch operation should fail immediately without initiating a page table walk.

<u>Implementation</u>**:**

- Modify the hardware or firmware to validate memory permissions before executing prefetch.

Part 2:

```
gil_roy@gpu-03:~/0450112_Cyber_lab/Lab4/ASLRLab$ python3 check.py 2a
make: Nothing to be done for 'all'.
Checking part 2A...
100%|
You passed 1000 of 1000 runs (100.0%)
Success! Good job

Your score is 10 / 10
You scored 100.0% for this part!
```

```
gil_roy@gpu-03:~/0450112_Cyber_lab/Lab4/ASLRLab$ python3 check.py 2b
make: Nothing to be done for 'all'.
Checking part 2B...
100%|
You passed 919 of 1000 runs (91.9%)
Success! Good job

Your score is 20 / 20
You scored 100.0% for this part!
gil_roy@gpu-03:~/0450112_Cyber_lab/Lab4/ASLRLab$ _
```

Part 3:

```
gil_roy@gpu-03:~/0450112_Cyber_lab/Lab4/ASLRLab$ python3 check.py 3
make: Nothing to be done for 'all'.
Checking part 3...
100%|
You passed 894 of 1000 runs (89.4%)
Success! Good job

Your score is 10 / 10
You scored 100.0% for this part!
gil_roy@gpu-03:~/0450112_Cyber_lab/Lab4/ASLRLab$
```