Page Cache – B

Objective: In this lab you will create a LKM called "cachetest" which will intercept (via kprobes) all calls to "add_to_page_cache" and "remove_from_page_cache()" and keep running counters to these calls.

File(s) for this lab:

Kprobes provide us with a powerful interface to intercept any kernel function before and after entry points. This allows us to inspect kernel functions, which might not be otherwise accessible via syscalls. "find_get_page" is an example of this. We need to use a Kprobe to access this routine since it lives only in kernel memory.

1. To use Kprobes include the header "kprobes.h". "pagecache.h" gives us access to the "add_to_page_cache_lru" and "delete_from_page_cache".

```
/* FocalPoint RHKI */
/* Lab15: Page Cache */
#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/init.h>

#include <linux/kprobes.h>
#include <linux/pagemap.h>

#define DRIVER_AUTHOR    "FocalPoint"
#define DRIVER_DESC      "Lab15b"
```

2. Declare some globals for holding the statistics for total accesses.

```
/* globals for stats */
int total_cache_add     = 0;
int total_cache_remove  = 0;
```

3. The routines to handle the Kprobe is as follows:

```
void handler_post_add(struct kretprobe_instance *ri, struct pt_regs *regs, unsigned long flags)
{
    total_cache_add++;
}

void handler_post_remove(struct kretprobe_instance *ri, struct pt_regs *regs, unsigned long flags)
{
    total_cache_remove++;
}
```

4. The kprobe structure needs the address or the name of the function to intercept.

```
static struct kprobe kp_add = {
        .pre_handler = NULL,
        .post_handler = handler_post_add,
        .fault_handler = NULL,

        .addr = (kprobe_opcode_t *) add_to_page_cache_lru,
};

static struct kprobe kp_remove = {
        .pre_handler = NULL,
        .post_handler = handler_post_remove,
        .fault_handler = NULL,

        .addr = (kprobe_opcode_t *) delete_from_page_cache,
};
```

5. Compile and run the module for a minute or so. Unload the module to see your results.

```
[ 1368.587447] cachetest: kprobes add_to_page_cache()/delete_from_page_cache() registered
[ 1399.145846] cachetest: kprobes unregistered
[ 1399.145851] cachetest: 3382 calls to add_to_page_cache() -- 3382 calls to delete_from_page_cache()
[user@localhost Lab15b]$
```