Check point Linux kernel Assignment

Task1:

1. A kernel module is code that can be dynamically loaded and unloaded into the kernel of the (linux) operating system without requiring a complete system reboot or recompile.
2. Dynamic Loading and Unloading: Kernel modules can be loaded and unloaded when we want, providing the flexibility to add or remove functionalities without restarting the whole system.
   Hardware Support: Kernel modules can be used to provide device drivers, enabling support for various hardware components without bloating the kernel with all possible drivers.
   Reduced Kernel Size: With kernel modules, less essential functionalities can be offloaded from the main kernel image, ant it is leading to a smaller and more streamlined core kernel.
3. Security Concerns: Kernel modules can have direct access to kernel internals, and it can lead to potential security risks when malicious modules are loaded into the kernel.
   Performance Overhead**:** Loading and unloading kernel modules can cause some performance overhead due to the additional process of loading code and resolving dependencies, so it can make your kernel slower.
4. A kernel module is an extension of the kernel itself. The kernel provides core functionalities, including process management, memory management, I/O, and system calls. It exposes APIs that can be accessed by kernel modules to interact with its internal services.

Check point Linux kernel Assignment

When a kernel module is loaded, it becomes part of the running kernel and can use these interfaces to extend the kernel's capabilities or modify its behavior.

5. The trivial example is device drivers. device drivers provides support for various hardware devices such as graphics cards, network cards, sound cards, and peripherals.
   One more example is Filesystems. Many filesystems, such as ext4, NTFS, and VFAT, are implemented as kernel modules to enable the operating system to interact with different file storage formats.
   We can talk also about Security Modules**:** Kernel modules can enhance system security by implementing access control policies, SELinux being one example.

Task2:

The code:

```c
#include <linux/init.h>
#include <linux/module.h>
#include <linux/kernel.h>

MODULE_LICENSE("GPL");
MODULE_AUTHOR("Asher&Shai");
MODULE_DESCRIPTION("A simple 'Hello worLd' Linux module.");
MODULE_VERSION("0.01");

static int __init lkm_hello_init(void) {
    printk(KERN_INFO "Hello, World!\n");
    return 0;
}

static void __exit lkm_by_exit(void) {
    printk(KERN_INFO "Goodbye, World!\n");
}

module_init(lkm_hello_init);
module_exit(lkm_by_exit);
```

Check point Linux kernel Assignment

The
dmesg:

```
[12331.192352] asher_shai_module: loading out-of-tree module taints kernel.
[12331.194925] asher_shai_module: module verification failed: signature and/or required key missing - tainting kernel
[12331.204210] Hello, World!
[12368.302074] Goodbye, World!
```

Task3:

The code:

me > shai-axelrod > cp_part2 > C asher_shai_module.c

```c
#include <linux/init.h>
#include <linux/module.h>
#include <linux/kernel.h>

MODULE_LICENSE("GPL");
MODULE_AUTHOR("Asher&Shai");
MODULE_DESCRIPTION("A simple 'Hello worLd' Linux module.");
MODULE_VERSION("0.01");

static char* input_var = "World";
module_param(input_var, charp, 0);
MODULE_PARM_DESC(input_var, "A character replacing the default 'world'");
static int __init lkm_hello_init(void) {
    printk(KERN_INFO "Hello, %s!\n", input_var);
    return 0;
}

static void __exit lkm_by_exit(void) {
    printk(KERN_INFO "Goodbye, %s!\n", input_var);
}

module_init(lkm_hello_init);
module_exit(lkm_by_exit);
```

The dmesg:

```
[15865.043311] Hello, shai axel!
[15950.536949] Goodbye, shai axel!
```

Check point Linux kernel Assignment

Task5: the code:

```c
include <linux/module.h>
#include <linux/netfilter.h>
#include <linux/ip.h>
#include <linux/netfilter_ipv4.h>
#include <linux/skbuff.h>

MODULE_LICENSE("GPL");
MODULE_AUTHOR("PrintIp");
MODULE_DESCRIPTION("ip addr printer");
MODULE_VERSION("0.01");


#define IPADDRESS(addr) \
    ((unsigned char *)&addr)[3], \
    ((unsigned char *)&addr)[2], \
    ((unsigned char *)&addr)[1], \
    ((unsigned char *)&addr)[0]
static struct nf_hook_ops *nf_printipaddr_ops = NULL;
static unsigned int nf_printipaddr_handler(void *priv, struct sk_buff *skb, const struct nf_hook_state *state)
{
    if (!skb) {
        return NF_ACCEPT;
    } else {
        char *sipStr = (char *)kmalloc(16, GFP_KERNEL); //container to the source ip
        char *dipStr = (char *)kmalloc(16, GFP_KERNEL); //container to the dest ip
        u32 sip;
        u32 dip;
        struct iphdr *iph; // the struct will contain data about the ip addr

        iph = ip_hdr(skb);
        sip = ntohl(iph->saddr); // get source ip address;
        dip = ntohl(iph->daddr); // get dest ip address;
        sprintf(sipStr, "%u.%u.%u.%u", IPADDRESS(sip)); // convert to standard IP address format
        sprintf(dipStr, "%u.%u.%u.%u", IPADDRESS(dip)); // convert to standard IP address format
        printk(KERN_INFO "the source ip addr is: %s\n", sipStr);
        printk(KERN_INFO "the dest ip addr is: %s\n", dipStr);
        return NF_ACCEPT;
    }
}
static int __init nf_printip_init(void)
{
    printk(KERN_INFO "start");
    nf_printipaddr_ops = (struct nf_hook_ops*)kcalloc(1, sizeof(struct nf_hook_ops), GFP_KERNEL);
    if (nf_printipaddr_ops != NULL) {
        nf_printipaddr_ops->hook = (nf_hookfn*)nf_printipaddr_handler; // the callback
        nf_printipaddr_ops->hooknum = NF_INET_PRE_ROUTING;  // register to the PRE_ROUTING hook
        nf_printipaddr_ops->pf = NFPROTO_IPV4; // the protocol

        nf_register_net_hook(&init_net, nf_printipaddr_ops); //register to the hook
    }
```

```c
    }
    return 0;
}

static void __exit nf_printip_exit(void) {
    if(nf_printipaddr_ops != NULL) {
        nf_unregister_net_hook(&init_net, nf_printipaddr_ops); //unrgister to the hook
        kfree(nf_printipaddr_ops);
    }
    printk(KERN_INFO "Exit");
}

module_init(nf_printip_init); //set nf_printip_init to run when the module is loaded
module_exit(nf_printip_exit); //set nf_printip_init to run when the module is removed
```

The output (dmesg):

Check point Linux kernel Assignment

```
22413.859078] the dest ip addr is: 192.168.48.128
22413.859948] the source ip addr is: 172.217.22.110
22413.859973] the dest ip addr is: 192.168.48.128
22413.864353] the source ip addr is: 172.217.22.110
22413.864593] the dest ip addr is: 192.168.48.128
22414.573797] the source ip addr is: 172.217.22.106
22414.573850] the dest ip addr is: 192.168.48.128
22414.582097] the source ip addr is: 172.217.22.106
22414.582147] the dest ip addr is: 192.168.48.128
22414.584157] the source ip addr is: 172.217.22.106
22414.584200] the dest ip addr is: 192.168.48.128
22414.584246] the source ip addr is: 172.217.22.106
22414.584287] the dest ip addr is: 192.168.48.128
22414.601341] the source ip addr is: 172.217.22.106
22414.601401] the dest ip addr is: 192.168.48.128
22414.646166] the source ip addr is: 172.217.22.106
22414.646222] the dest ip addr is: 192.168.48.128
22414.681126] the source ip addr is: 172.217.22.106
22414.681172] the dest ip addr is: 192.168.48.128
22414.681951] the source ip addr is: 172.217.22.106
22414.681994] the dest ip addr is: 192.168.48.128
22414.691185] the source ip addr is: 172.217.22.106
22414.691231] the dest ip addr is: 192.168.48.128
22414.692158] the source ip addr is: 172.217.22.106
22414.692217] the dest ip addr is: 192.168.48.128
22414.693032] the source ip addr is: 172.217.22.106
22414.693290] the dest ip addr is: 192.168.48.128
22414.697078] the source ip addr is: 172.217.22.106
22414.697123] the dest ip addr is: 192.168.48.128
22416.206509] the source ip addr is: 34.107.221.82
22416.206558] the dest ip addr is: 192.168.48.128
22416.717205] the source ip addr is: 34.107.221.82
22416.717259] the dest ip addr is: 192.168.48.128
22416.752965] the source ip addr is: 34.120.208.123
22416.753016] the dest ip addr is: 192.168.48.128
22416.755014] the source ip addr is: 34.120.208.123
22416.755059] the dest ip addr is: 192.168.48.128
22416.755105] the source ip addr is: 34.120.208.123
22416.755146] the dest ip addr is: 192.168.48.128
```