Networks and Systems Security
Assignment 1

The Kernel Module:

The kernel module code starts by including the relevant header files.

We thereafter create a global hook structure and set the module license (and optionally, the author, description and version).

We then define a function (in my case, *hook_func*) which will be called as soon as a packet is received. In *hook_func*, we check which protocol the packet is sent using. We take different actions depending on what protocol the packet was sent using and/or which flags are set:

- ICMP protocol (e.g. ping): We drop it
- TCP protocol:
    - No flag is set (Null scan): We drop it
    - Only ACK is set (Ack scan): We drop it
    - Only FIN is set (Fin scan): We drop it
    - URG, RST & FIN are set (Xmas scan): We drop it
    - Any other flag permutation: We accept it
- For all other protocols (e.g. UDP): We accept it

We thereafter define the init function which runs as soon as the kernel module starts (in my case, *init_lkm*) where we set the relevant parameters of the hook data structure while we make sure we set the *hook* parameter to *hook_func* (the function we declared earlier). We register the hook and return.

We then move forward to the exit function which runs when we terminate the kernel module (in my case, *exit_lkm*) where we

deregister the hook and free the memory occupied by the global hoot structure.

At the end of the file, we then set the init and exit functions to *init_lkm* and *exit_lkm* respectively using *module_init()* and *module_exit()* respectively.

How to Run:

We must simply keep the makefile and the module in the same directory and run *make* which compiles the code as a kernel module and generates the *.so* extension file (in addition to others) which is the actual module binary.

The module can be run by typing *insmod lkm.so* and stopped by typing *rmmod lkm*. In the interim, we can look at the messages being printed by the kernel module by looking at the kernel log using the *dmesg* command.

Test Script:

The test script is simply a set of 4 nmap commands with varying flags that make it run null, fin, ack and xmas scans respectively:

nmap -sN 192.168.182.130
nmap -sF 192.168.182.130
nmap -sA 192.168.182.130
nmap -sX 192.168.182.130

The script (*test.sh*) can be run by simply doing *chmod +x test.sh* to give execute permission and *./test.sh*.