LAB 7
A20453991

Task 2:

Yes, an attacker can use the backdoor exposed by the rootkit to remotely get access. Rootkit program which is installed as a kernel module(which makes it run at kernel privilege level) can open backdoor TCP ports and thereby granting remote access to attackers through bind shell or reverse shell.

Instead of adding a device file, we can have a rootkit that lives in the master boot loader. This allows rootkit to do anything before OS runs.

Also, once the attacker gains the control of the system and creates a bind shell and runs it as a background process, the rootkit can then hide the information about this bind shell.

Task 3:

(1) If the rootkit wants to use routines that live inside the kernel, it has to call kallsyms_*() API with the symbol name to get the pointer of that function. This is why we need function pointers and kallsyms_*() functions.

(2) For hiding, we need to modify read handler function but kernel won't allow you to do so by making these data structures read only even in kernel mode. Hence if kernel tries to modify them, an exception will be raised. To overcome this, we need to turn off the write protection and override and then turning write protection on. Here write protection bit is present in cr0. Hence, we need to go through these for overriding handler functions.

We can have a rootkit that lives in the master boot loader. This allows rootkit to do anything before OS runs. This way, rootkit can be loaded every time system reboots.

Task 4:

Algorithm for this:

1. We need to get the init_net.proc_net's rb_node and search for rb_node named tcp and then get the data of it to remove the line that contains port 9474.
2. rb_node's content can be found using rb_entry function
3. A function hook_tcp4_seq_show on the similar lines of hook_pid_maps_seq_show can be created to modify show handler with new function by unprotecting the page first , changing the handler and then protecting it again
4. We can create a function hide_tcp_show (similar to hide_seq_show)that actually hides the string that contains port 9474.
4. Adding deinittcpshow function to change back everything to normal state.

Although, this is high level algorithm, this covers almost everything that has to be done for attack to work. I tried implementing the above but unfortunately couldn’t resolve the errors.