Ian Talla 10/30/2019

CSE 331 – StackSmashingUltimate Plans for the Rootkit

Our overall plan:

- insert custom modules wherever the natural functions exits  
- locate syscall table  
- highjack write syscall to not display our modules  
- modify syscall memory page to disable write protect  
- create our own write function

- change ls, ps to hide specific files using the above

We are using Linux 2.4 so that we can directly edit the syscall files

We are using C, naturally, so that we can edit the syscal directly, hijack write syscall

Ian: Work on the ls part

Matthew:

Nicholas:

Kevin