The kernel module, rather than being a single piece of flowing code, is currently a large collection of snippets of network oriented code. It was difficult finding resources, libraries, and protocols that allow for the type of analysis we are aiming for and were also available to C based kernel modules (in fact, finding them has been the bulk of the work for this part of the project so far), but we've discovered some useful tools. Our module currently contains snippets that utilize the sys/socket.h and the linux.netfilter.h libraries to carry out an array of tasks such as checking for the availability of ports, tallying incoming and outgoing packets and analyzing their protocols, source IP addresses, and destination IP addresses, and…