# Manual Exploitation - Kioptrix

For the manual exploitation, he does a walkthrough for the exploitation of the "mod_ssl/2.8.4" service. Refer to the "Scanning & Enumaration" notebook, in the "Researching Potential Vulnerabilities" section, I exploit the service using the same exploit.

Turns out that the systax provided in the Read.me file was correct. I used the wrong Offset when using that syntax.

Heath explain what the exploit is doing based on the output provided during the exploit.

Post-exploitation, first touch.

The first thing we need to do is discover our Ip address, routing table, arp table, we wanna see if the machine is dual homed. If the machine has two NICs, then we could move to this second NIC to discover this new network that we did not have access before.