# Using Snort to Stop Brute Force Attack

1. TryHackMe simulated a Brute Force Attack
2. I opened the terminal and entered the command, “sudo snort -dev -l .” to allow snort to sniff and log the packets.
3. After 1 minute, I stopped the sniffing and opened the snort log.
4. When investigating the log, it became apparent that port 22, SSH, was being exploited due to many packets containing powershell code.
5. I also noticed that port 4444, which is a common Metasploit port, was being used to send information out of the machine.
6. To stop this I created two snort rules that blocked inbound communication from port 22 and outbound communication from port 4444.