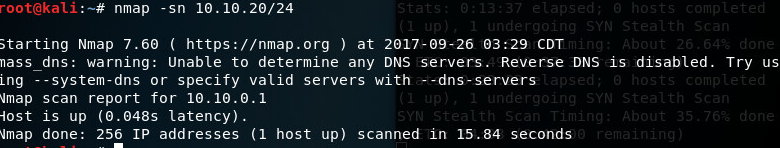
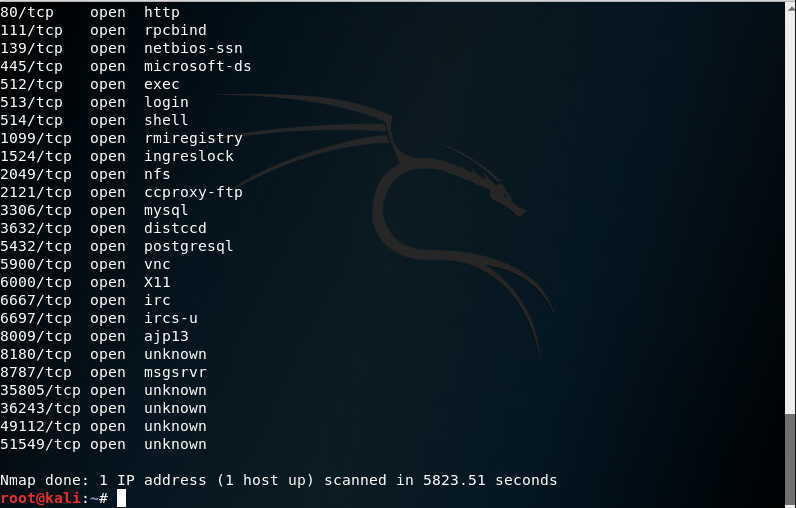
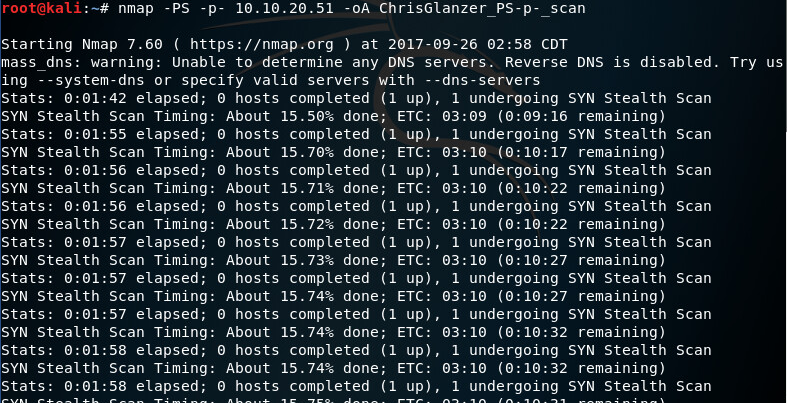
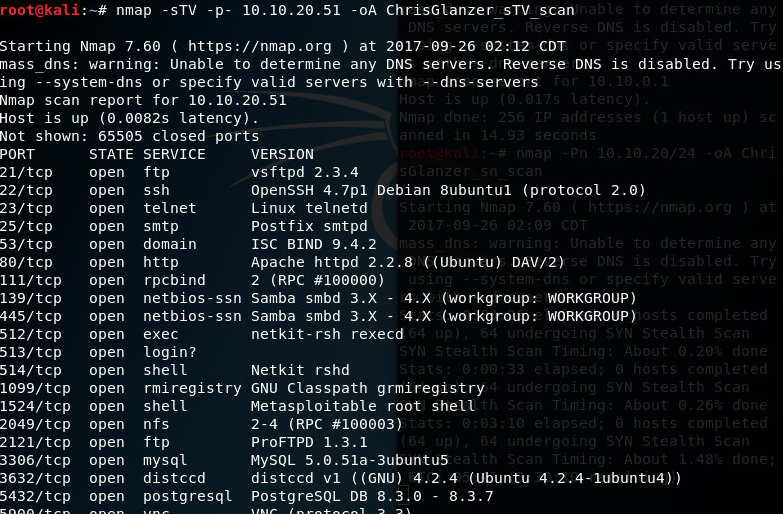
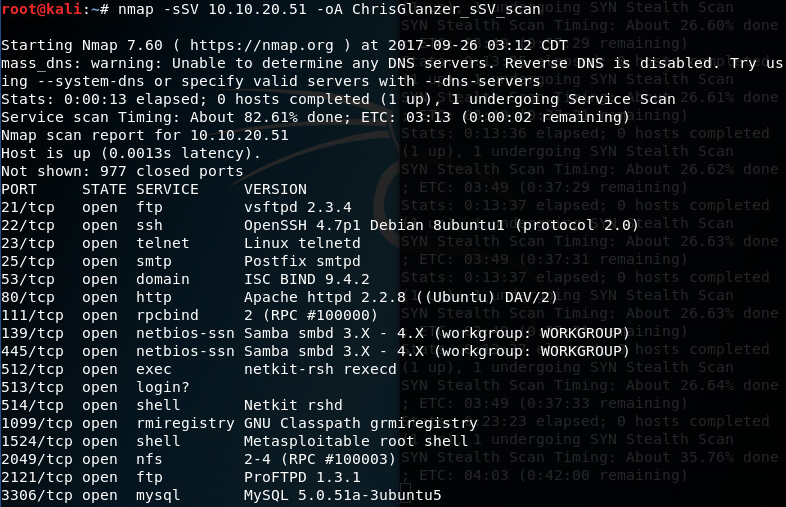
1. All output files attatched in a zip
2. a pure Ping scan scan revealed little going on on the network, so I used a TCP connect scan to sweep the network and bring up a few other devices, (the metasploitable was among them at 10.10.20.51) among others (5 total live boxes)
3. this was followed by a full port scan of all 65k+ ports on the box as well as
4.   
   (the TCP ACK scan above)
5. We finished with a TCPSYN Sweep on the same device
6. A couple of other ways to discover hosts would include (sT scans as we used in place of sn when it failed) PR Scans (arp scans) which turned up nothing, complaining of reverse dns being disabled… meaning that our device isn’t on the same subnet as the target range…
7. What we could gather from this session is that the Box is a Debian Ubuntu box (ssh version, port 22), with a number of exposed systems, like the apache http server which is currently not updated to the latest (2.4.27) version, as well as their MySQL database… the Box Is clearly defined as a metsaploitable box by the (1524) “metasploitable root shell.”