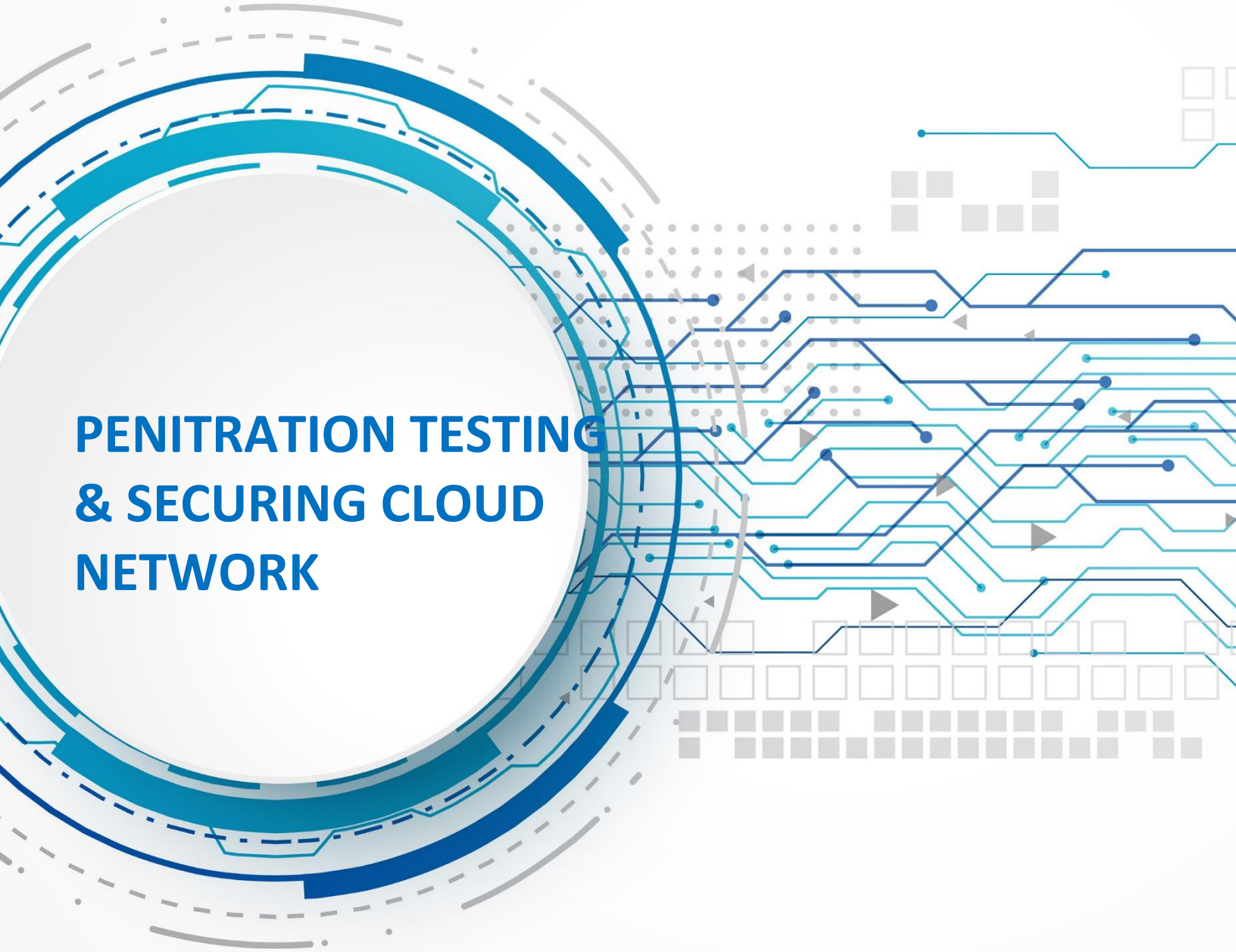


PENITRATION TESTING & SECURING CLOUD NETWORK

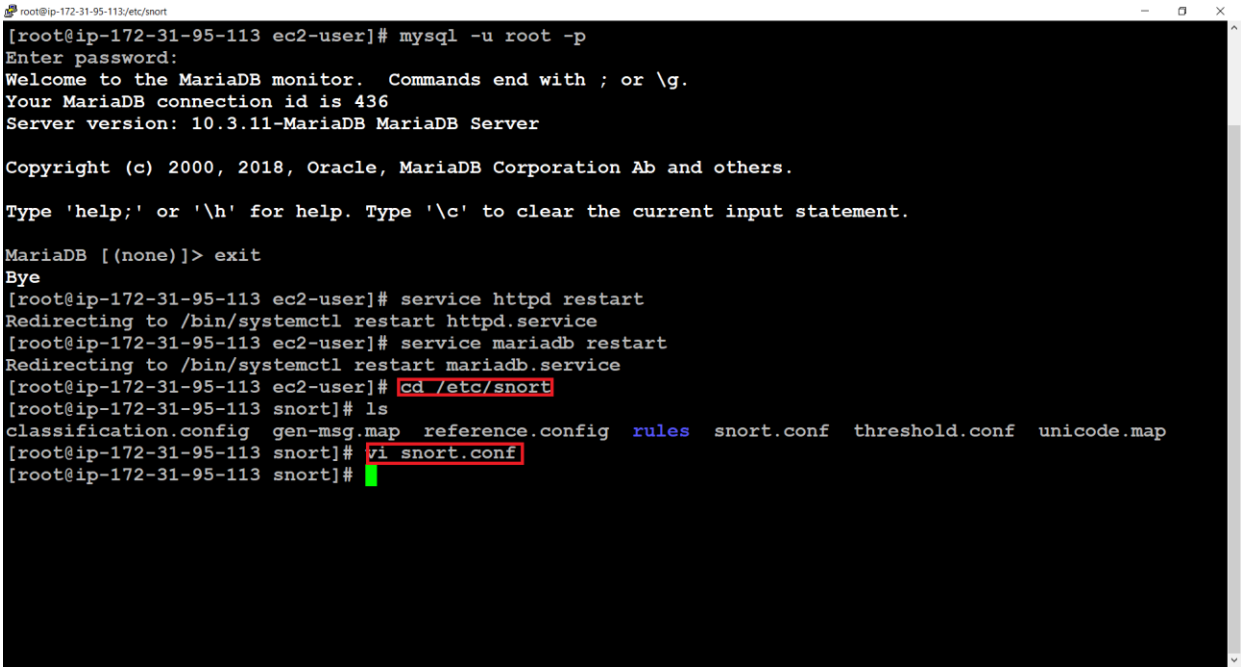
R0HIT GUPTA

SECURITY

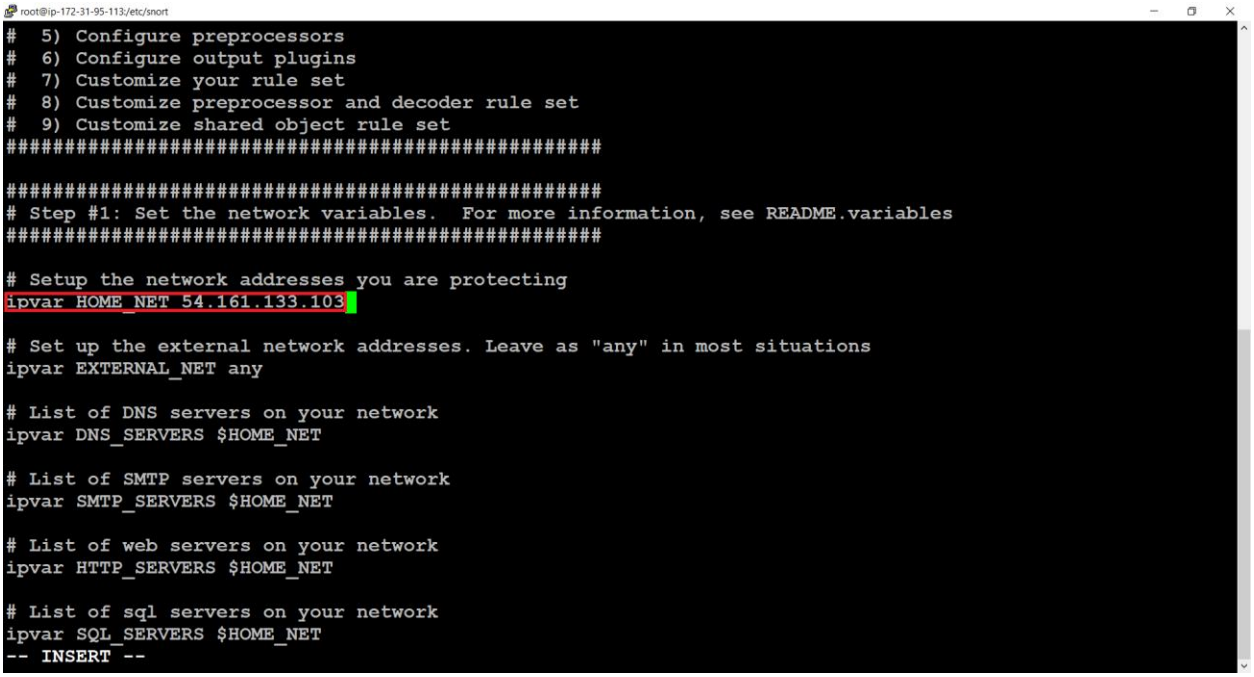
SNORT

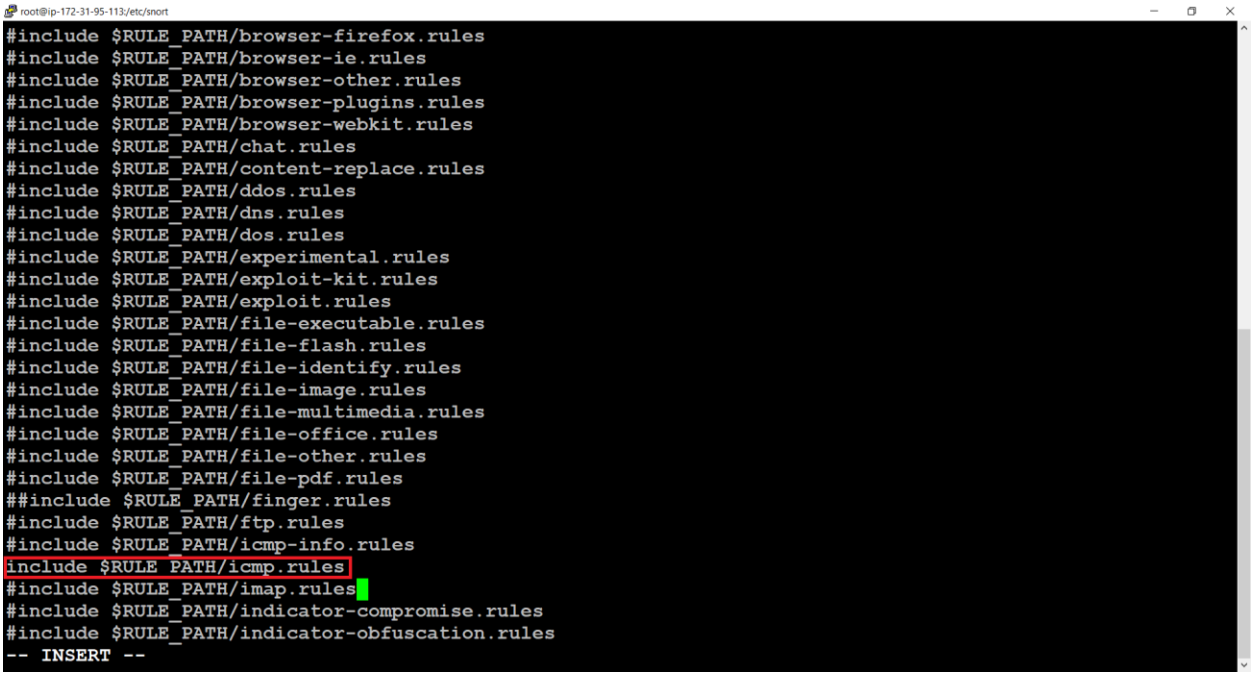
Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) created in 1998 by Martin Roesch, founder and former CTO of Sourcefire. Snort is now developed by Cisco, which purchased Sourcefire in 2013, at which Roesch is a chief security architect.

INSTALLING SNORT REPOSITORIES AND PACKAGES

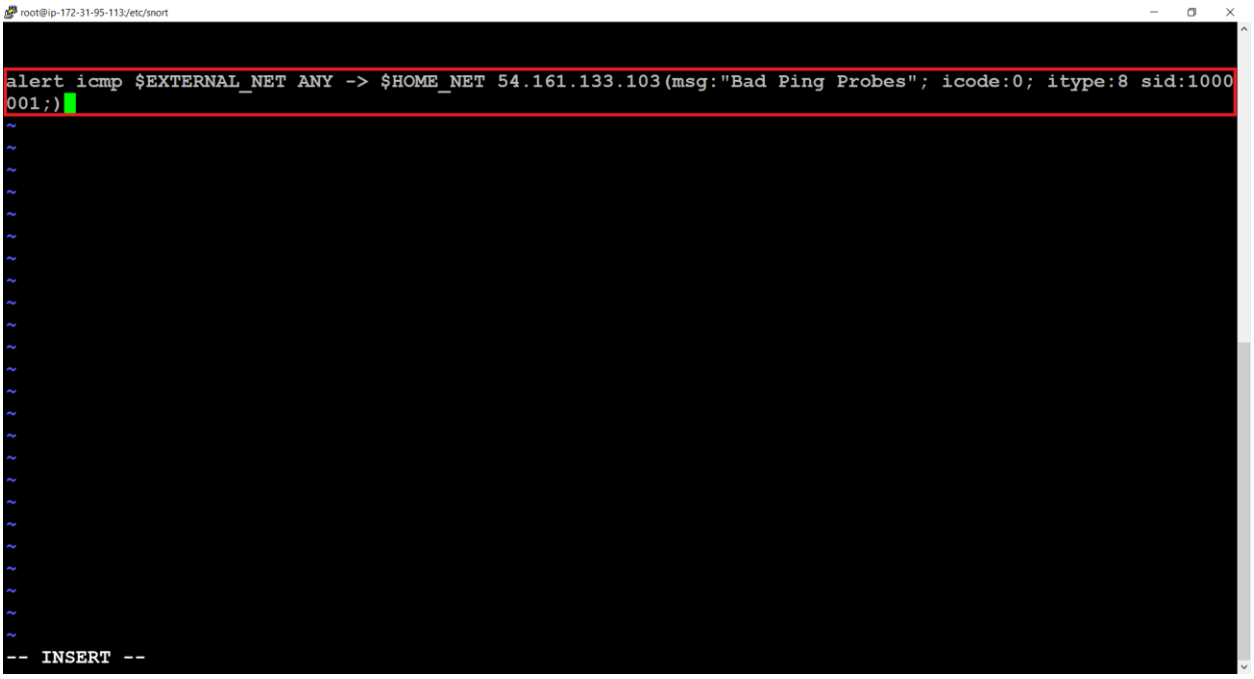


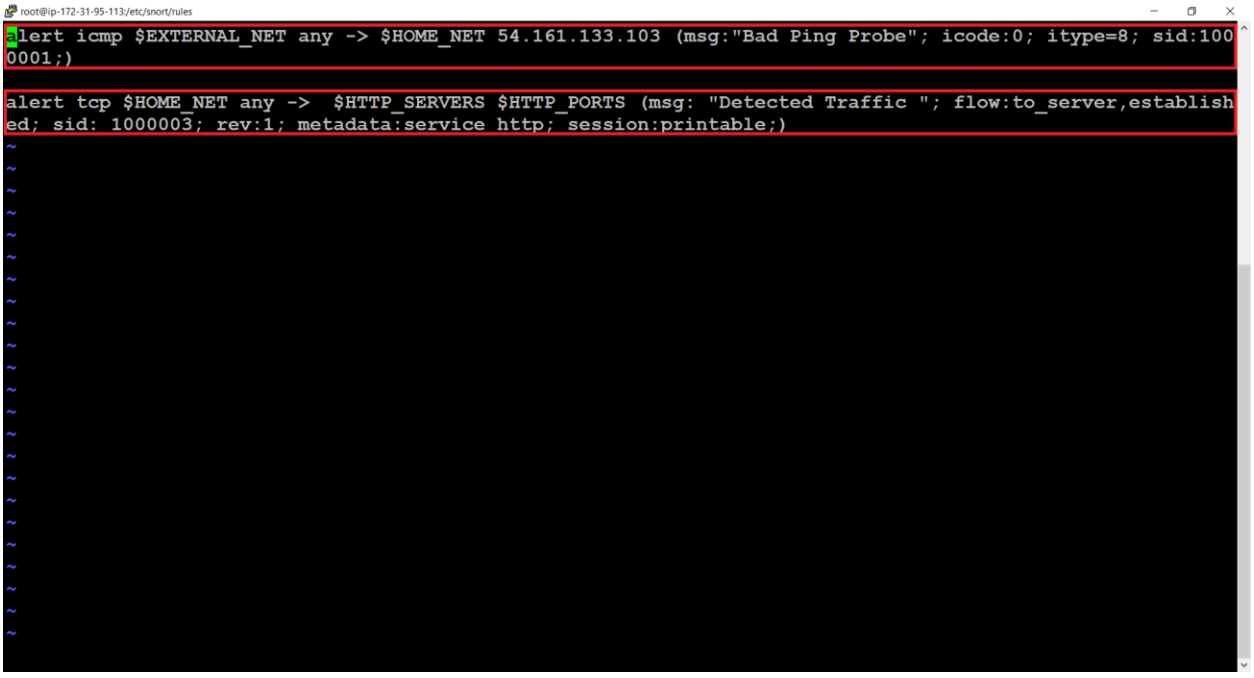
CONFIGURING SNORT



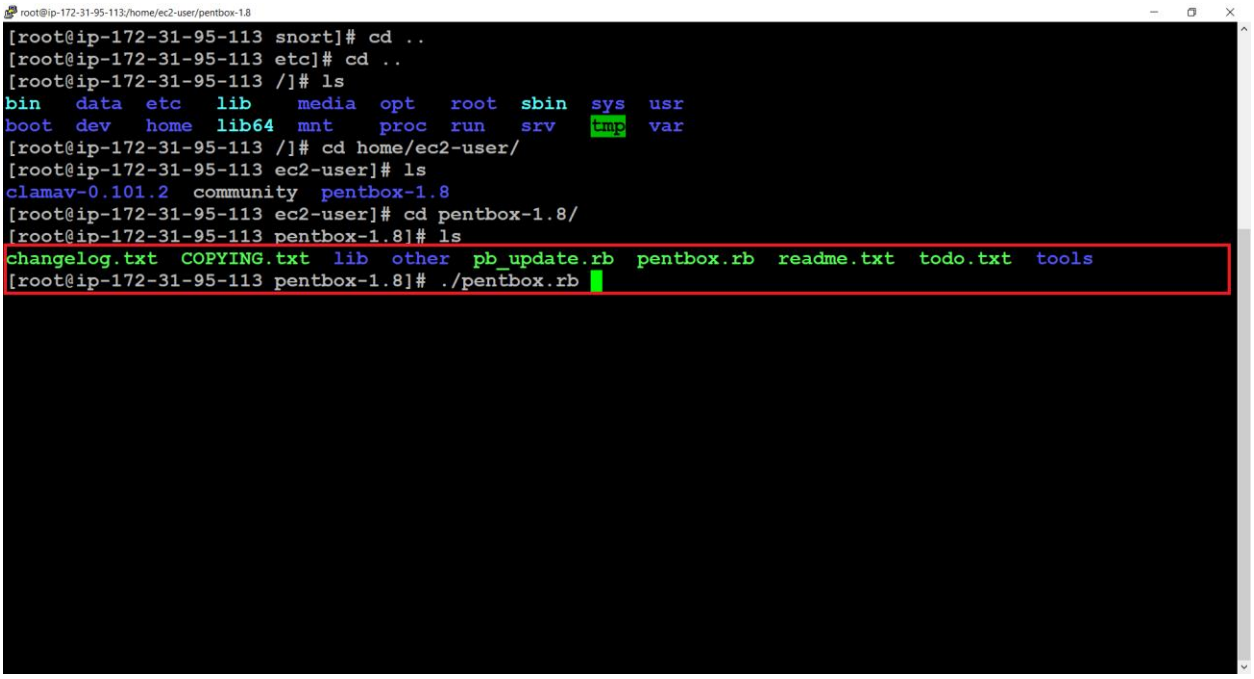


CONFIGURING THE RULES FOR ICMP AND HTTP

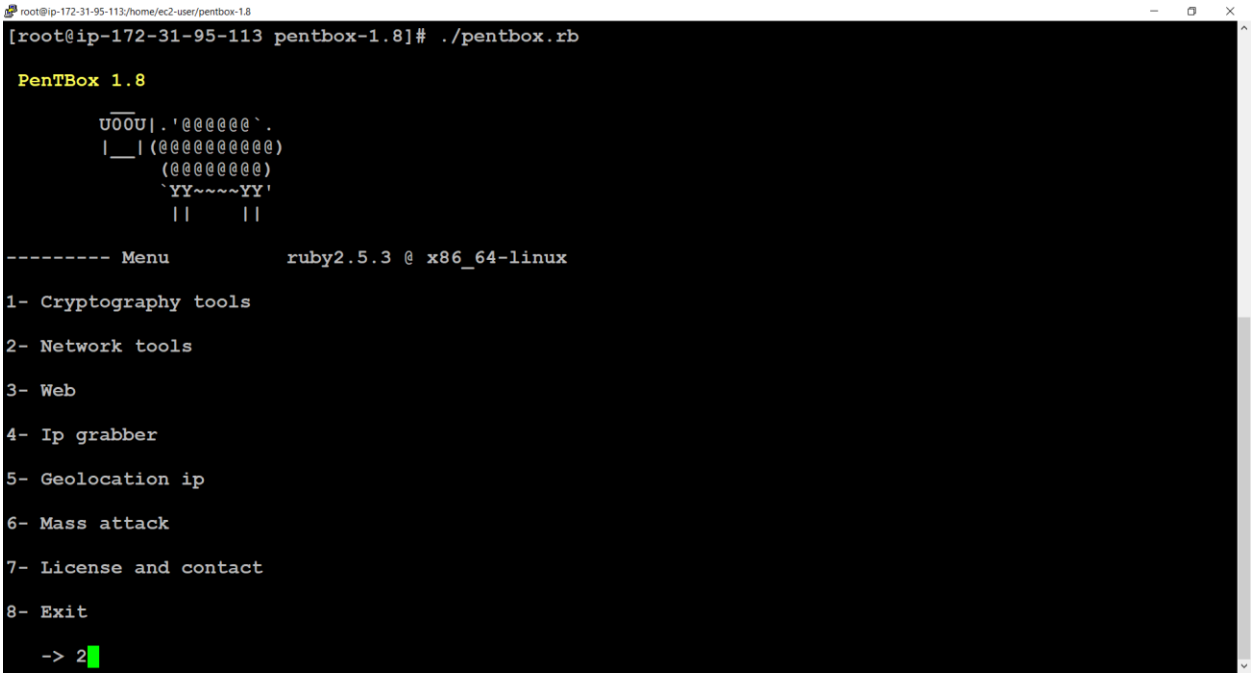


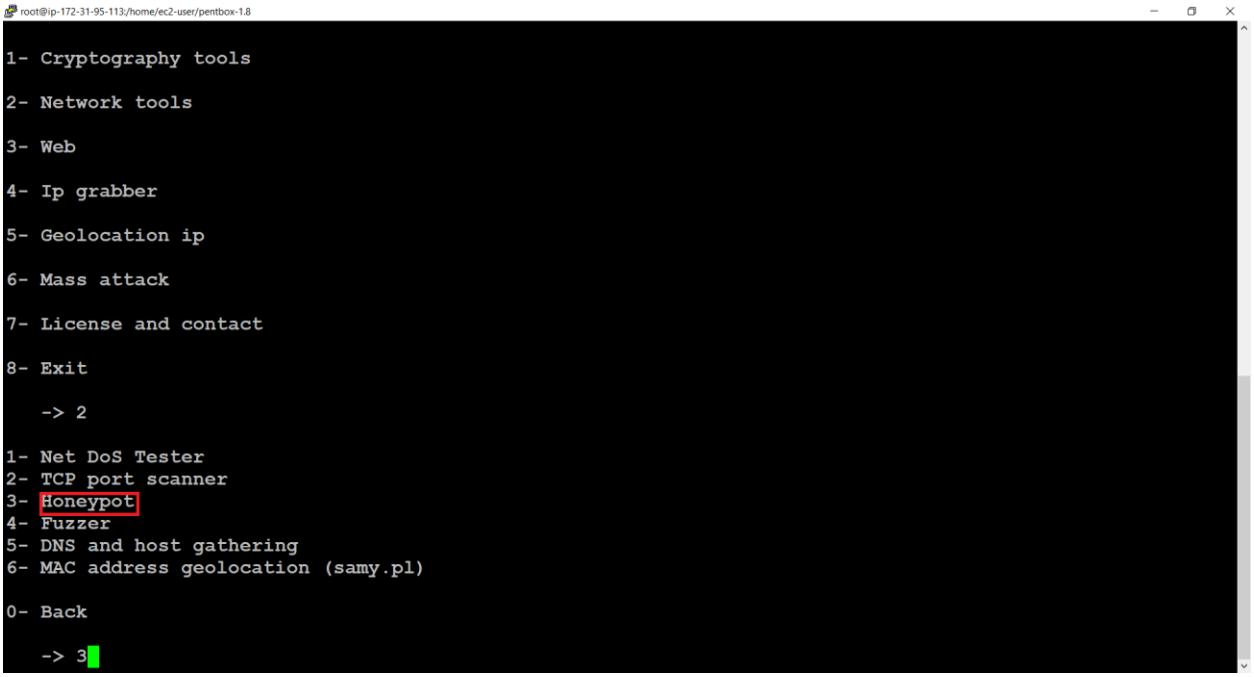


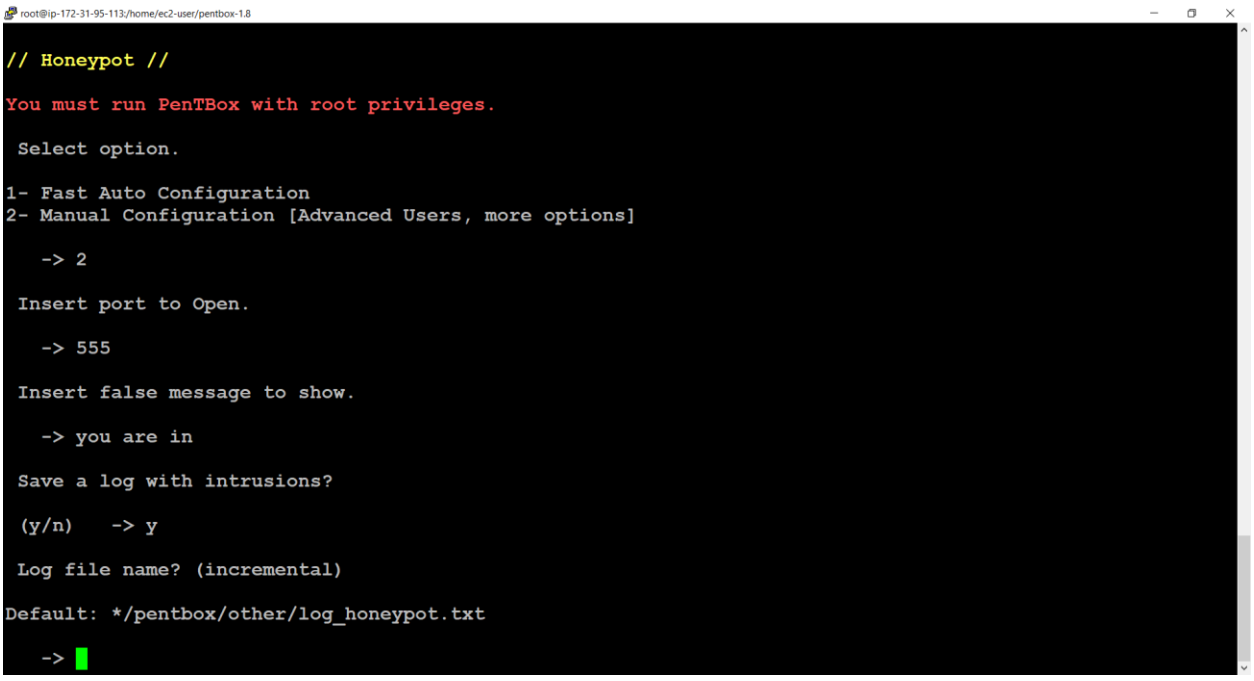
INSTALLING AND CONFIGURING HONEYPOT

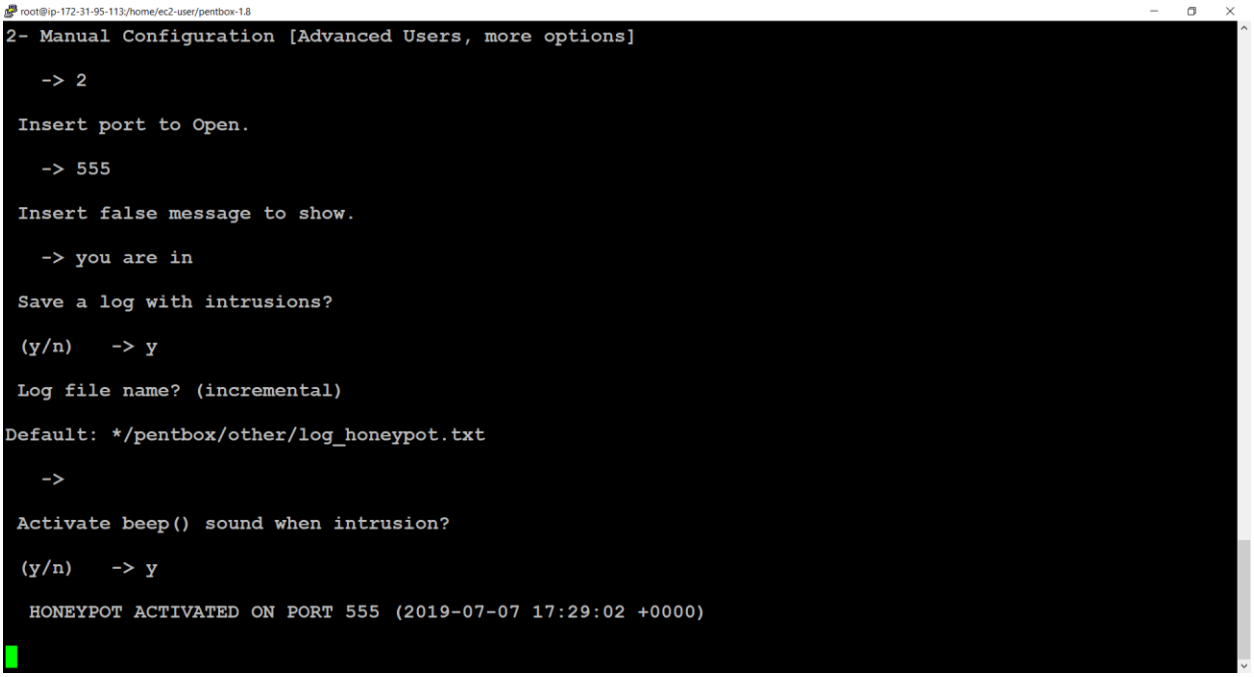


>>PentBox




root@ip-172-31-95-113:/home/ec2-user/pentbox-1.8
1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8- Exit
-> 2
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)
0- Back
-> 3


root@ip-172-31-95-113:/home/ec2-user/pentbox-1.8
// Honeypot //
You must run PenTBox with root privileges.
Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
-> 2
Insert port to Open.
-> 555
Insert false message to show.
-> you are in
Save a log with intrusions?
(y/n) -> y
Log file name? (incremental)
Default: */pentbox/other/log_honeypot.txt
->



>>After implementing honeypot