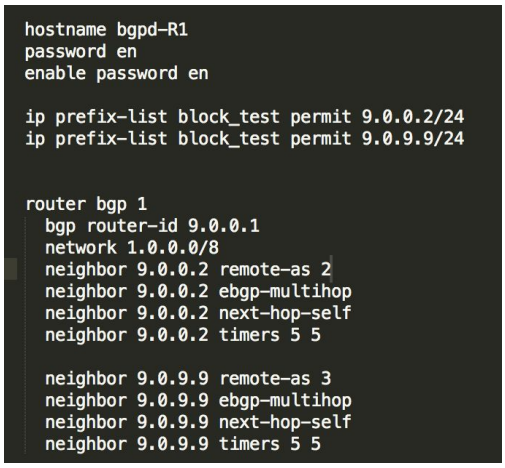
1. The solution to avoid the attack altogether is based on the ip prefix permissions, effectively I whitelist only the prefixes that are a part of the conf files, once we whitelist those anything outside will be blocked. Using only the permit option instead of the deny option means we don't have to hard code for the specific prefix we are trying to avoid and allows us to generalize outside of that prefix as well.

2. With the exception of bgpd-R6.conf I altered every bgpd-* file in the configuration directory, each with their permits for their prefixes, I did this at each node, so we would not be dependant on a single AS, but any one of them could be used. (bgpd-R1.conf, bgpd-R2.conf, bgpd-R3.conf, bgpd-R4.conf, bgpd-R5.conf)

3. As explained above the new conf files are almost exactly the same as the ones in part 3 except for the addition of the permits, a sample for bgpd-R1.conf is shown below:

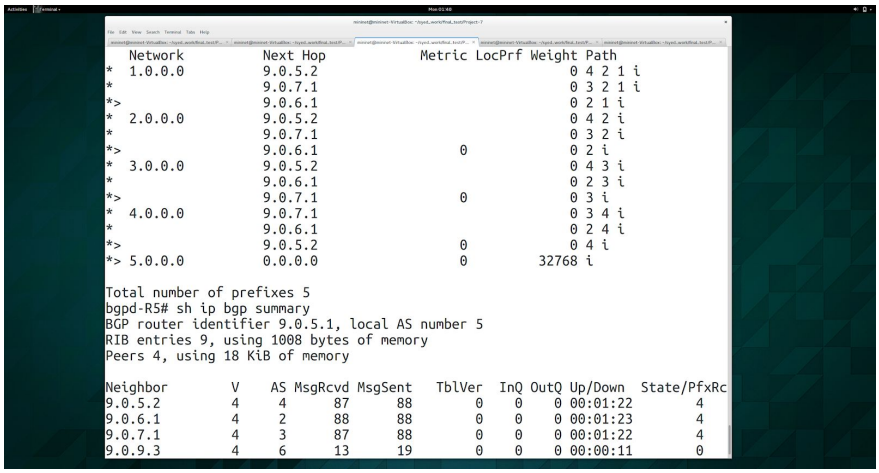


```
hostname bgpd-R1
password en
enable password en

ip prefix-list block_test permit 9.0.0.2/24
ip prefix-list block_test permit 9.0.9.9/24


router bgp 1
  bgp router-id 9.0.0.1
  network 1.0.0.0/8
  neighbor 9.0.0.2 remote-as 2
  neighbor 9.0.0.2 ebgp-multihop
  neighbor 9.0.0.2 next-hop-self
  neighbor 9.0.0.2 timers 5 5

  neighbor 9.0.9.9 remote-as 3
  neighbor 9.0.9.9 ebgp-multihop
  neighbor 9.0.9.9 next-hop-self
  neighbor 9.0.9.9 timers 5 5
```

   As you can see the file looks very similar except for the two added lines, which I named "block_test" and permits the two prefixes that are connected to R1. This is the same for all the altered files listed in part 2 depending on the number of prefixes connected.

4. The instructions for using this updated code is 100% identical to the original process:
   a. Sudo python bgp.py
   b. (New Tab) ./connect.sh
   c. (New Tab) ./website.sh
   d. (New Tab) ./start_rogue.sh or ./stop_rogue.sh

5. If done correctly, the user should be able to run steps a-c identically and see the same results, for step d, instead of seeing **<h1>*** Attacker web server ***</h1>** and an update in the tab from step b, you will see the same **<h1>Default web server</h1>**



You can see that 9.0.9.3 isn’t idle, but also that it can’t connect meaning it has been stopped from attacking.