<u>HOW TO PREVENT DDOS ATTACK ON CENTOs 7</u>

CentOS DDoS protection – A guide to secure your server from DDoS!

DDoS(Distributed Denial Of Service) is an advanced version of DoS(Denial Of Service).

1. SSH HARDNING

Create a new user: in terminal as root

- **adduser** someWeirdName
- **passwd** someWeirdName (to create password for new user) to generate Password, you can use LastPass.com.

Disable root remote login: in ssh

nano /etc/ssh/sshd_config (edit following line)

- Port 22 (change to your desire port in 32)
- LoginGraceTime 2m
- PermitRootLogin no (disable remote root logins)
- StrictModes yes (to add extra layer of security)
- after creating username and password (**make sure the user can login**)
- MaxAuthTries 6 (maximum number of authentication attempts permitted per connection)
- MaxSessions 10 (maximum number of open sessions per connection)
- `systemctl reload sshd or service sshd reload`

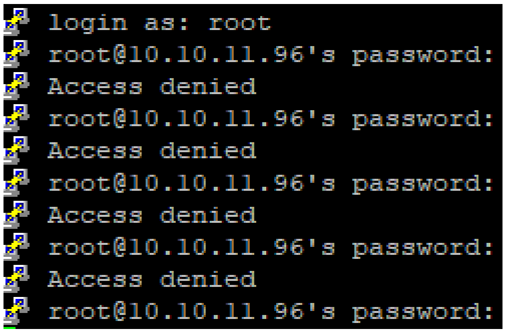
Tell semanage to effect new port

- semanage port -a -t ssh_port_t -p tcp #PORTNUMBER

Install semanage

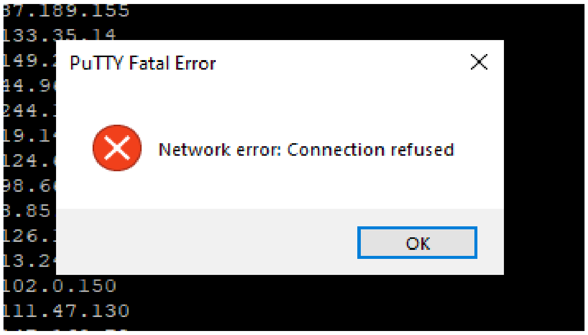
- yum -y install policycoreutils-python (install policycoreutils-python)
- nano /etc/hosts.allow (list all allowed network)
- nano /etc/hosts.deny (list all denyed network)

root login deny



```
login as: root
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
```

trying to login with port 22

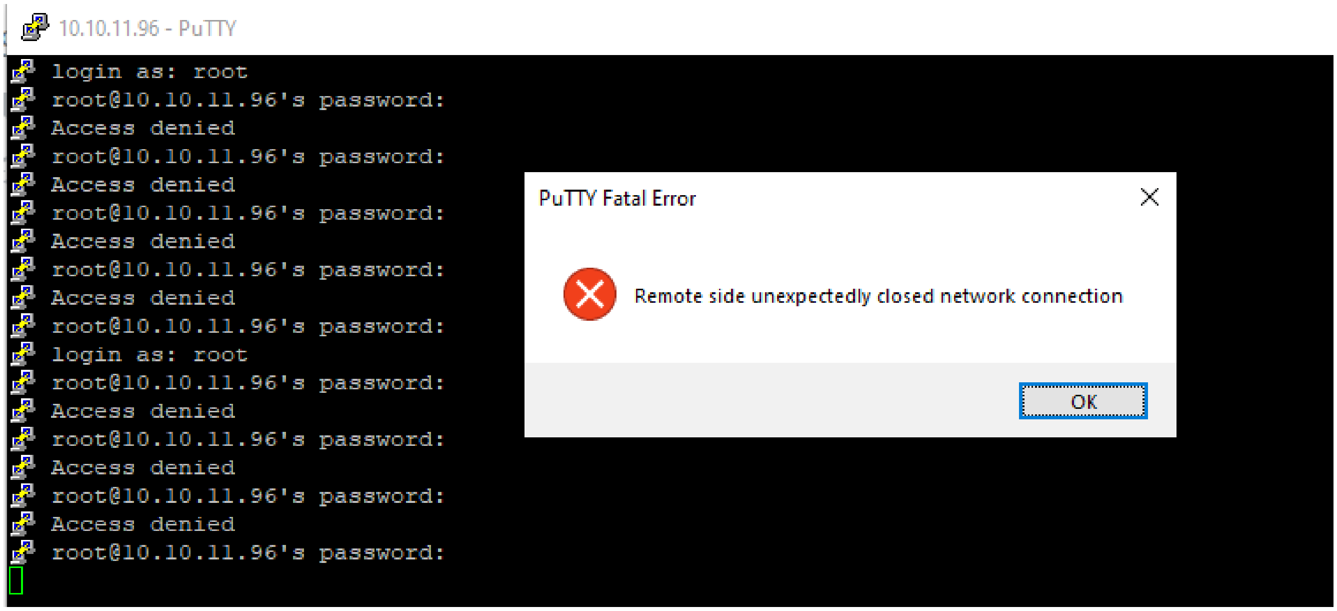


```
37.189.155
133.35.14
149.
44.9
244.
19.1
124.
98.6
3.85
126.
13.2
102.0.150
111.47.130
```

PuTTY Fatal Error

Network error: Connection refused

at 9th try of root and correct password (connection was closed)



```
login as: root
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
login as: root
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
Access denied
root@10.10.11.96's password:
```

Remote side unexpectedly closed network connection