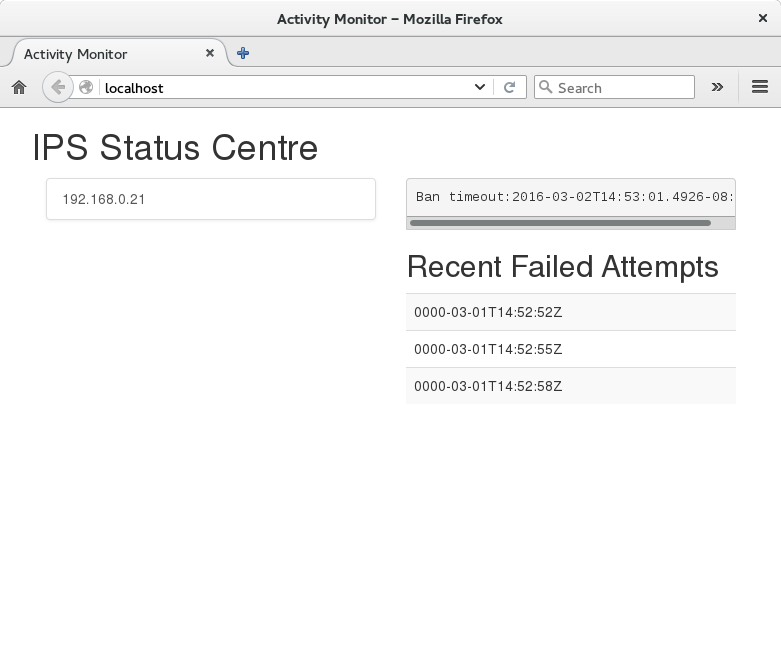
|  |
| --- |
| Mar 1 14:52:50 datacomm sshd[4085]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.0.21 user=root  Mar 1 14:52:50 datacomm sshd[4085]: pam\_succeed\_if(sshd:auth): requirement "uid >= 1000" not met by user "root"  Mar 1 14:52:52 datacomm sshd[4085]: Failed password for root from 192.168.0.21 port 55724 ssh2  Mar 1 14:52:53 datacomm sshd[4085]: pam\_succeed\_if(sshd:auth): requirement "uid >= 1000" not met by user "root"  Mar 1 14:52:55 datacomm sshd[4085]: Failed password for root from 192.168.0.21 port 55724 ssh2  Mar 1 14:52:56 datacomm sshd[4085]: pam\_succeed\_if(sshd:auth): requirement "uid >= 1000" not met by user "root"  Mar 1 14:52:58 datacomm sshd[4085]: Failed password for root from 192.168.0.21 port 55724 ssh2  Mar 1 14:52:59 datacomm sshd[4085]: Connection closed by 192.168.0.21 [preauth] |



|  |
| --- |
| Chain INPUT (policy ACCEPT)  target prot opt source destination  [root@datacomm COMP8006.IPS]# iptables -L  DROP all -- 192.168.0.21 anywhere  Chain FORWARD (policy ACCEPT)  target prot opt source destination  DROP all -- 192.168.0.21 anywhere  Chain OUTPUT (policy ACCEPT)  target prot opt source destination  DROP all -- 192.168.0.21 anywhere |

MODIFIED THE TIMEOUT IN THE MANIFEST

|  |
| --- |
| [root@datacomm COMP8006.IPS]# iptables -L  Chain INPUT (policy ACCEPT)  target prot opt source destination  Chain FORWARD (policy ACCEPT)  target prot opt source destination  Chain OUTPUT (policy ACCEPT)  target prot opt source destination |