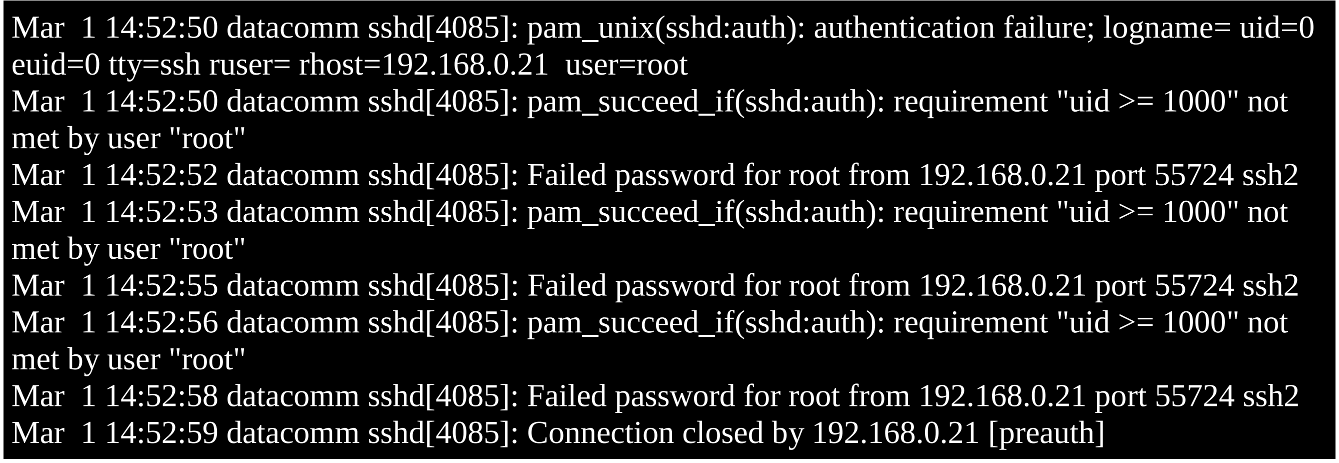
Testing Doc

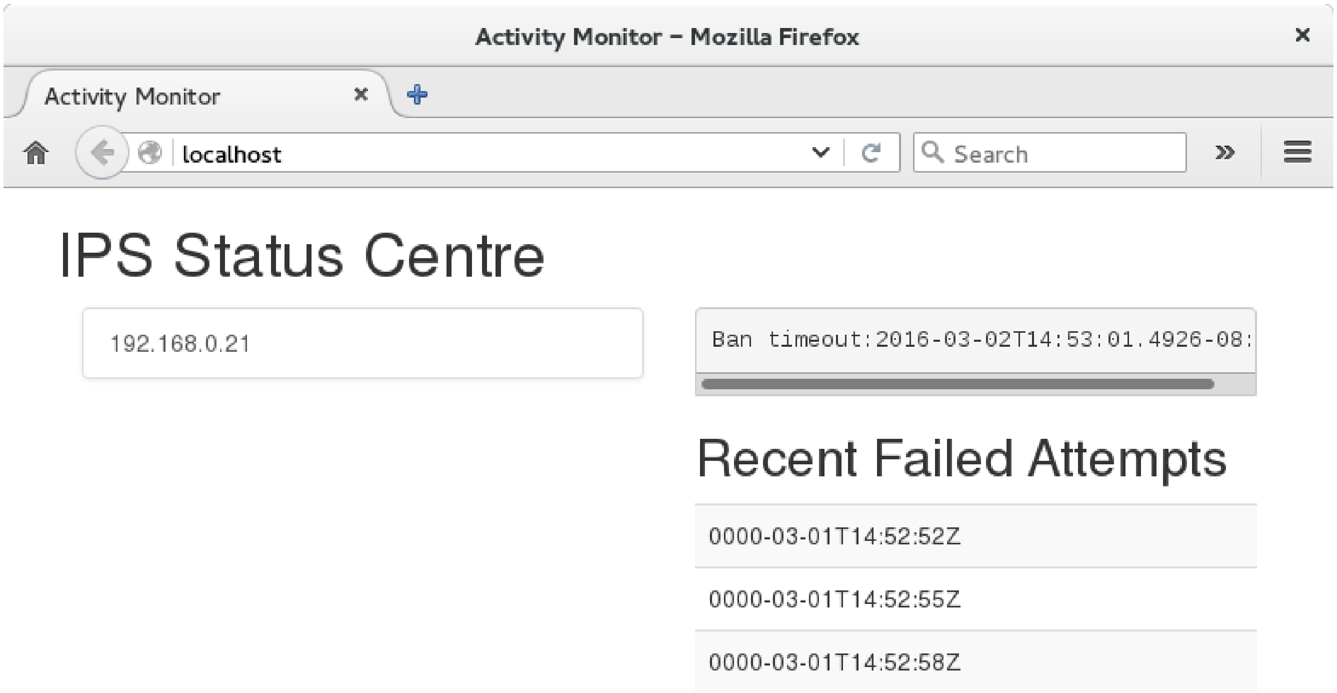
Test	Tool	Result	Passed	
Attempted to log into the machine with the IPS 3 times successively. Should get banned by IPS	SSH/iptables	Remote host banned successfully	Yes	Fig 1, 2, 3
Information about attempted connections displayed on webpage	Firefox	Shows details about ban, including expiry time.	Yes	Fig 2
Users are unbanned after 1 day of being banned	iptables	User was unbanned when the ban expired	Yes	Fig 4
User should not be banned for less than 3 attempted connections in 1 minute	iptables	Success	Yes	Fig 5, 6

Figure 1:



```
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]
```

Figure 2



IPS Status Centre

192.168.0.21

```
Ban timeout:2016-03-02T14:53:01.4926-08:
```

Recent Failed Attempts

0000-03-01T14:52:52Z

0000-03-01T14:52:55Z

0000-03-01T14:52:58Z

Figure 3

```
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
```

Figure 4

```
[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
```

Fig 5:

```
Mar  1 14:53:40 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 14:52:53 datacomm sshd[4085]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
Mar  1 14:52:56 datacomm sshd[4085]: Failed password for root from 192.168.0.21 port 55724 ssh2
Mar  1 14:52:57 datacomm sshd[4085]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
```

Fig 6:

```
[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
```