Following describes steps to setup new sshd users –

Overview – We will have two ssh daemons running on the hosts one on 22 which will be configured to allow access to our team and second one on 2222 to allow ops users login which will only have access to Profile teller login screen.

Setup Steps

1)    Create a fresh sshd config for port 2222

[root@prfdvedevit01 ssh]# cat sshd\_p2222\_config

# V 1.0 This is developed by Profile IPS to regulate the OPS user logins

Port 2222

Protocol 2

PasswordAuthentication yes

UsePAM yes

#

ClientAliveInterval 900

#

PidFile /var/run/sshd-2222.pid

ForceCommand /p6059/drv

2)    Create service file to start sshd using sshd\_p2222\_config in /usr/lib/systemd/system

Note that this is copied from original sshd service file and changed ExecStart to use the config file for port#2222 also have added dependency to start this service after sshd on port 22 starts

[root@prfdvedevit01 system]# cat sshd\_p2222.service

[Unit]

Description=OpenSSH second server daemon on p2222

Documentation=man:sshd(8) man:sshd\_config(5)

After=network.target sshd-keygen.service sshd.service

Wants=sshd-keygen.service

[Service]

Type=notify

EnvironmentFile=/etc/sysconfig/sshd

ExecStart=/usr/sbin/sshd -D -f /etc/ssh/sshd\_p2222\_config $OPTIONS

ExecReload=/bin/kill -HUP $MAINPID

KillMode=process

Restart=on-failure

RestartSec=42s

RestartPreventExitStatus=255

[Install]

WantedBy=multi-user.target

3)    Run following command to allow sshd bind to port#2222 . by default selinux prevents starting ssh deamon on ports other than 22

# semanage port -a -t ssh\_port\_t -p tcp 2222

 verify using :

 # semanage port -l | grep ssh\_port\_t

ssh\_port\_t                     tcp      2222, 22

4)    Enable sshd\_p2222 service and start it

[root@prfdvedevit01 system]# systemctl enable sshd\_p2222

Created symlink from /etc/systemd/system/multi-user.target.wants/sshd\_p2222.service to /usr/lib/systemd/system/sshd\_p2222.service.

[root@prfdvedevit01 system]# systemctl start sshd\_p2222

[root@prfdvedevit01 system]#

[root@prfdvedevit01 system]# systemctl status sshd\_p2222

â— sshd\_p2222.service - OpenSSH second server daemon on p2222

   Loaded: loaded (/usr/lib/systemd/system/sshd\_p2222.service; enabled; vendor preset: disabled)

   Active: active (running) since Tue 2017-06-13 23:51:46 EDT; 9s ago

     Docs: man:sshd(8)

           man:sshd\_config(5)

 Main PID: 20828 (sshd)

   CGroup: /system.slice/sshd\_p2222.service

           â””â”€20828 /usr/sbin/sshd -D -f /etc/ssh/sshd\_p2222\_config

Jun 13 23:51:46 prfdvedevit01 systemd[1]: Starting OpenSSH second server daemon on p2222...

Jun 13 23:51:46 prfdvedevit01 sshd[20828]: Could not load host key: /etc/ssh/ssh\_host\_dsa\_key

Jun 13 23:51:46 prfdvedevit01 sshd[20828]: Server listening on 0.0.0.0 port 2222.

Jun 13 23:51:46 prfdvedevit01 sshd[20828]: Server listening on :: port 2222.

Jun 13 23:51:46 prfdvedevit01 systemd[1]: Started OpenSSH second server daemon on p2222.

[root@prfdvedevit01 system]# netstat -anp | grep sshd

tcp        0      0 0.0.0.0:2222            0.0.0.0:\*               LISTEN      20828/sshd

tcp        0      0 0.0.0.0:22              0.0.0.0:\*               LISTEN      8010/sshd

tcp        0      0 10.206.206.146:22022    10.206.206.250:59294    ESTABLISHED 7959/sshd: ec2-user

tcp6       0      0 :::2222                 :::\*                    LISTEN      20828/sshd

tcp6       0      0 :::22                   :::\*                    LISTEN      8010/sshd

5)    Now sshd deamon is running on ports 22 and 2222 , but when someone logs in using port 2222 we are forcing them to run only command specified in “ForceCommand” option in case of this poc which is /p6059/drv . As this command or script runs in the forked shell intr or exit or kill of this particular results in falling back to server where ssh command was initiated

Login to server on port 22

[ec2-user@prfbvebvt10 ~]$ ssh 10.206.206.146