

linux ssh How to Hide the OpenSSH Version Details when Telnet to Port 22

Article Number: 668 | Rating: Unrated | Last Updated: Wed, Apr 22, 2020 10:30 AM

Information

How to hide the OpenSSH version details when telnet to port 22 in Red Hat Enterprise Linux?

Details

OpenSSH version details are displayed from the file **/usr/sbin/sshd**. The only method to hide the version detail is to edit the binary file **/usr/sbin/sshd** and remove/overwrite the appropriate line.

Steps:

1. Copy the file **/usr/sbin/sshd** to **/tmp**.

```
#cp /usr/sbin/sshd /tmp  
#ksh -o vi
```

2. Find the location of text **OpenSSH** in it using strings command.

Look for text **SSH-2.0-OpenSSH_4.x** since it is the version showed in telnet output.

```
#cd /tmp
#strings -t d -a -n 7 sshd | grep -i openssh
308104 OpenSSH_4.3p2-FC-4.3p2-36.el5_4.2
310376 hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160
@openssh.com,hmac-sha1-96,hmac-md5-96
310768 OpenSSH_4.3p2
311452 OpenSSH_4.3
```

3. Remove 311452 OpenSSH_4.3 line from the above output using dd command.

```
#dd if=./sshd bs=1 skip=311452 count=11 | od -A n -c
11+0 records in
11+0 records out
11 bytes (11 B) copied, 0.000929952 seconds, 11.8 kB/s
O p e n S S H _ 4 . 3
#dd if=./sshd bs=1 count=311452 of=sshd.1
311452+0 records in
311452+0 records out
311452 bytes (311 kB) copied, 3.77178 seconds, 82.6 kB/s
#dd if=./sshd bs=1 skip=311452 count=11 of=sshd.2
11+0 records in
11+0 records out
11 bytes (11 B) copied, 0.000568408 seconds, 19.4 kB/s
#dd if=./sshd bs=1 skip=311463 count=999999999 of=sshd.3
96889+0 records in
96889+0 records out
96889 bytes (97 kB) copied, 1.69652 seconds, 57.1 kB/s
OpenSSH_4.3 is now cut and copied to sshd.2 file.
```

4. Check the content of sshd.2 file using the od command.

```
#od -A n -c sshd.2
O p e n S S H _ 4 . 3
```

5. Write the text **ItsHidden** to sshd.2 and check the file size change before and after.

```
#ls -l sshd.2
-rw-r--r-- 1 root root 11 May  6 14:11 sshd.2
```

```
#print -n ItsHidden > sshd.2
#ls -l sshd.2
-rw-r--r-- 1 root root 11 May  6 14:12 sshd.2
```

6. Combine all the above sshd files to **sshd.new**.

```
#cat sshd.* > sshd.new
```

7. Give execute permission **sshd.new** and replace the sshd binary with **sshd.new**.

```
#chmod 755 ./sshd.new
#cp /usr/sbin/sshd /usr/sbin/sshd.bak
#rm /usr/sbin/sshd
#cp /tmp/sshd.new /usr/sbin/sshd
```

8. Restart sshd service and test the outcome with telnet command.

```
#service sshd stop
#ps aux | grep -i sshd
#kill -9 <pid_sshd>
#service sshd restart
#telnet localhost 22
```

Posted - Wed, Apr 22, 2020 10:30 AM. This article has been viewed 5622 times.

Online URL: <http://kb.ictbanking.net/article.php?id=668>