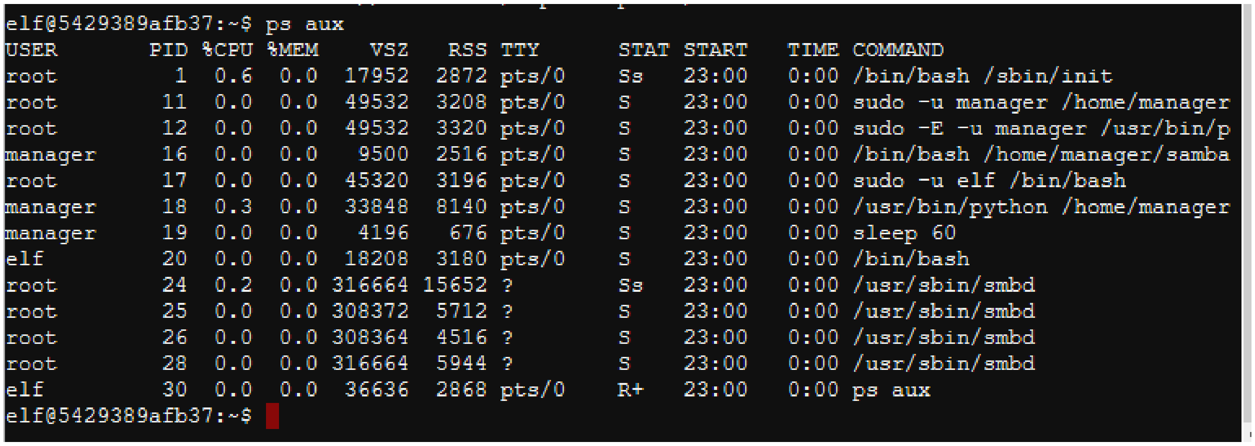
Terminal--Stall Mucking Report (part 2)

The Password

The terminal is running Linux, so the command we want should be the standard `ps aux`. That command roughly the equivalent of the task list in Windows. More information can be found here.

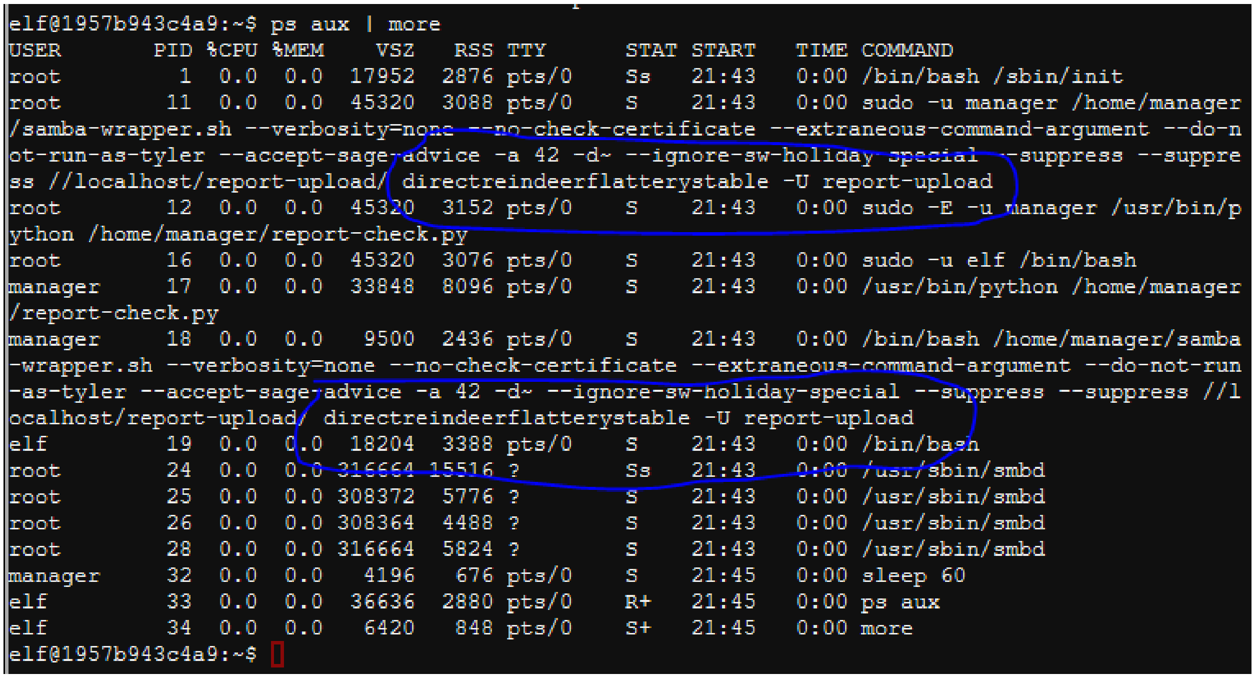
One problem is that `ps aux` by itself does not show the entire command line unless it is very short. You can get the entire command by piping the output into `less`. Since less is blocked, we'll use `more`.

This does not help much (`ps aux`)



```
elf@5429389afb37:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.6  0.0  17952  2872 pts/0    Ss   23:00   0:00 /bin/bash /sbin/init
root        11  0.0  0.0  49532  3208 pts/0    S    23:00   0:00 sudo -u manager /home/manager
root        12  0.0  0.0  49532  3320 pts/0    S    23:00   0:00 sudo -E -u manager /usr/bin/p
manager     16  0.0  0.0   9500  2516 pts/0    S    23:00   0:00 /bin/bash /home/manager/samba
root        17  0.0  0.0  45320  3196 pts/0    S    23:00   0:00 sudo -u elf /bin/bash
manager     18  0.3  0.0  33848  8140 pts/0    S    23:00   0:00 /usr/bin/python /home/manager
manager     19  0.0  0.0   4196   676 pts/0    S    23:00   0:00 sleep 60
elf         20  0.0  0.0  18208  3180 pts/0    S    23:00   0:00 /bin/bash
root        24  0.2  0.0 316664 15652 ?        Ss   23:00   0:00 /usr/sbin/smbd
root        25  0.0  0.0 308372  5712 ?        S    23:00   0:00 /usr/sbin/smbd
root        26  0.0  0.0 308364  4516 ?        S    23:00   0:00 /usr/sbin/smbd
root        28  0.0  0.0 316664  5944 ?        S    23:00   0:00 /usr/sbin/smbd
elf         30  0.0  0.0  36636  2868 pts/0    R+   23:00   0:00 ps aux
elf@5429389afb37:~$
```

This does help (`ps aux | more`).



```
elf@1957b943c4a9:~$ ps aux | more
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  17952  2876 pts/0    Ss   21:43   0:00 /bin/bash /sbin/init
root        11  0.0  0.0  45320  3088 pts/0    S    21:43   0:00 sudo -u manager /home/manager
/samba-wrapper.sh --verbosity=none --no-check-certificate --extraneous-command-argument --do-n
ot-run-as-tyler --accept-sage-advice -a 42 -d~ --ignore-sw-holiday-special --suppress --suppre
ss //localhost/report-upload/ directreindeerflatterystable -U report-upload
root        12  0.0  0.0  45320  3152 pts/0    S    21:43   0:00 sudo -E -u manager /usr/bin/p
ython /home/manager/report-check.py
root        16  0.0  0.0  45320  3076 pts/0    S    21:43   0:00 sudo -u elf /bin/bash
manager     17  0.0  0.0  33848  8096 pts/0    S    21:43   0:00 /usr/bin/python /home/manager
/report-check.py
manager     18  0.0  0.0   9500  2436 pts/0    S    21:43   0:00 /bin/bash /home/manager/samba
-wrapper.sh --verbosity=none --no-check-certificate --extraneous-command-argument --do-not-run
-as-tyler --accept-sage-advice -a 42 -d~ --ignore-sw-holiday-special --suppress --suppress //l
ocalhost/report-upload/ directreindeerflatterystable -U report-upload
elf         19  0.0  0.0  18204  3388 pts/0    S    21:43   0:00 /bin/bash
root        24  0.0  0.0 316664 15516 ?        Ss   21:43   0:00 /usr/sbin/smbd
root        25  0.0  0.0 308372  5776 ?        S    21:43   0:00 /usr/sbin/smbd
root        26  0.0  0.0 308364  4488 ?        S    21:43   0:00 /usr/sbin/smbd
root        28  0.0  0.0 316664  5824 ?        S    21:43   0:00 /usr/sbin/smbd
manager     32  0.0  0.0   4196   676 pts/0    S    21:45   0:00 sleep 60
elf         33  0.0  0.0  36636  2880 pts/0    R+   21:45   0:00 ps aux
elf         34  0.0  0.0   6420   848 pts/0    S+   21:45   0:00 more
elf@1957b943c4a9:~$
```

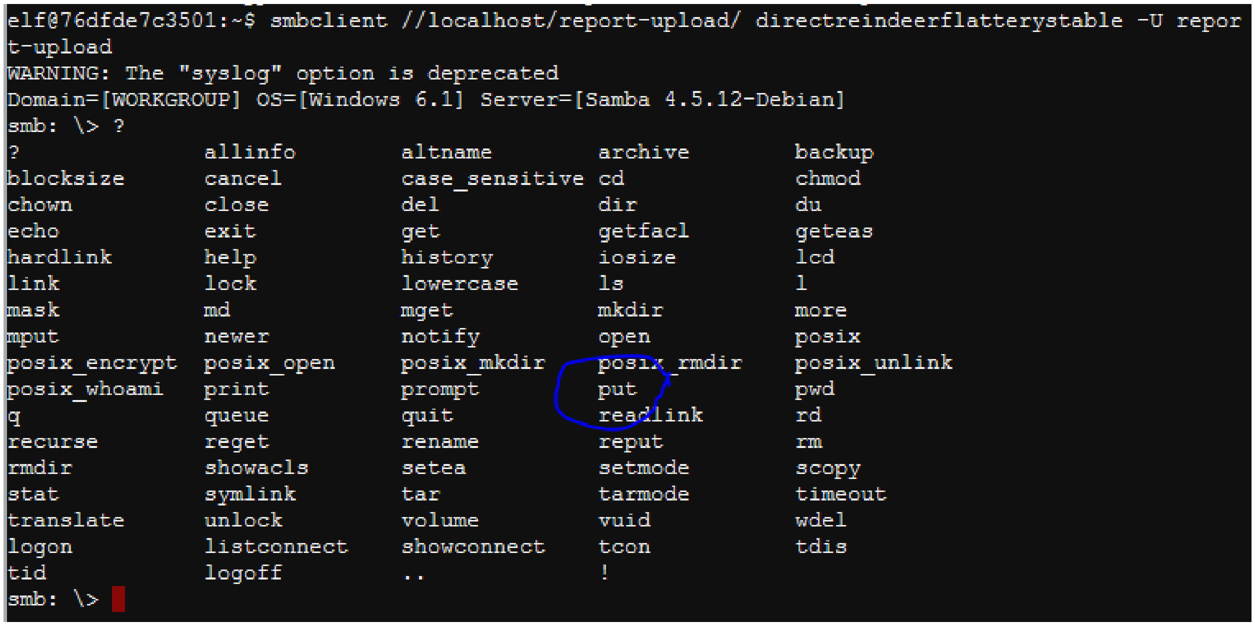
The script is using the user name `report-upload` and the password `directreindeerflatterystable`.

Accessing the File Share

This article is a basic guide to using Samba (the executable is called `smbclient`.) A simple way to connect to a share is

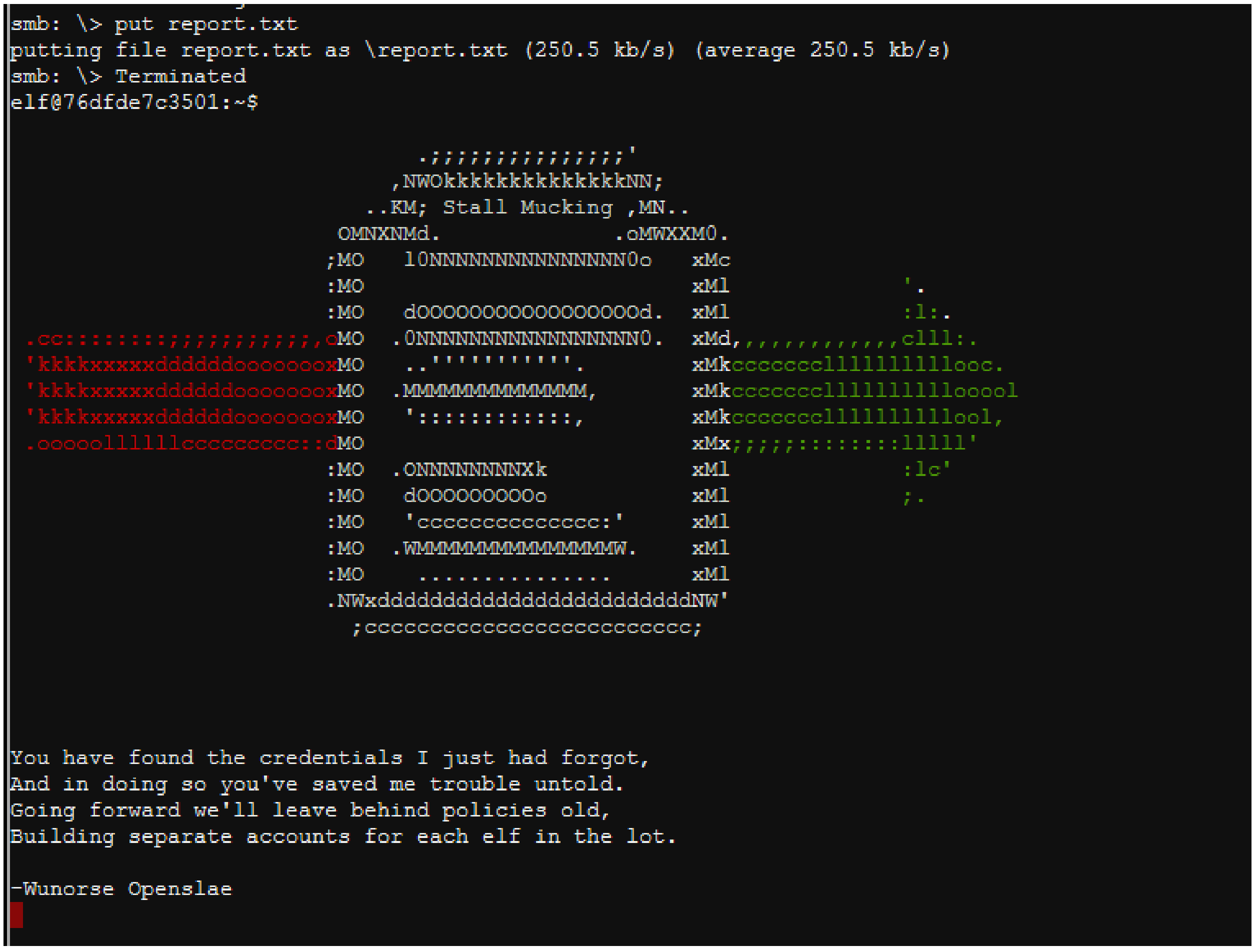
```
smbclient //localhost/report-upload/ directreindeerflatterystable -U report-upload
```

The -U gives the user name and the password is just there by itself. The “?” brings up help.



```
elf@76dfde7c3501:~$ smbclient //localhost/report-upload/ directreindeerflatterystable -U repor
t-upload
WARNING: The "syslog" option is deprecated
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.5.12-Debian]
smb: \> ?
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            dir            du
echo           exit           get            getfacl        geteas
hardlink       help           history        iosize         lcd
link           lock           lowercase      ls             l
mask           md             mget           mkdir          more
mput           newer          notify         open           posix
posix_encrypt  posix_open     posix_mkdir    posix_rmdir    posix_unlink
posix_whoami   print          prompt         put            pwd
q              queue          quit           readlink       rd
recurse        reget          rename         reput          rm
rmdir          showacls       setea          setmode        scopy
stat           symlink        tar            tarmode        timeout
translate      unlock         volume         vuid           wdel
logon          listconnect    showconnect    tcon           tdis
tid            logoff         ..             !
smb: \>
```

The next thing we need is `put`, as in put `report.txt`



```
smb: \> put report.txt
putting file report.txt as \report.txt (250.5 kb/s) (average 250.5 kb/s)
smb: \> Terminated
elf@76dfde7c3501:~$

                               .;;;;;;;;;;;;;;;;'
                             ,NWOkkkkkkkkkkkkkkkNN;
                           ..KM; Stall Mucking ,MN..
                         OMNXNMd.             .oMWXXM0.
                        ;MO   l0NNNNNNNNNNNNNNNN0o  xMc
                        :MO                         xMl             '.
                        :MO   dOOOOOOOOOOOOOOOOOd.  xMl             :l:.
 .cc::::::::;;;;;;;;;;;,oMO  .0NNNNNNNNNNNNNNNNNN0. xMd,,,,,,,,,,,,,clll:.
 'kkkxxxxxxddddddoooooooxMO   ..''''''''''''.       xMkccccccclllllllllllooc.
 'kkkxxxxxxddddddoooooooxMO  .MMMMMMMMMMMMMM,       xMkcccccccllllllllllooool
 'kkkxxxxxxddddddoooooooxMO   ':::::::::::::,       xMkccccccclllllllllllool,
 .ooooollllllccccccccc::dMO                         xMx;;;;;::::::::lllll'
                        :MO  .ONNNNNNNNNXk          xMl             :lc'
                        :MO   dOOOOOOOOOOo          xMl             ;.
                        :MO   'ccccccccccccccc:'    xMl
                        :MO  .WMMMMMMMMMMMMMMMMW.   xMl
                        :MO     ...............     xMl
                        .NWxdddddddddddddddddddddddddNW'
                          ;cccccccccccccccccccccccccc;



You have found the credentials I just had forgot,
And in doing so you've saved me trouble untold.
Going forward we'll leave behind policies old,
Building separate accounts for each elf in the lot.

-Wunorse Openslae
```

Up Next

Talk to Wunorse now that you have fixed his problem, and he will give you hints in his dialog and on your badge. We will need them to complete the Data Repo Analysis Challenge.