

Rexec Service

```
512/tcp open  exec      syn-ack netkit-rsh rexecd  
513/tcp open  login     syn-ack  
514/tcp open  tcpwrapped syn-ack  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Rexec is a legacy service on UNIX / Linux systems which allows users to execute commands remotely

Rexec Service

```
512/tcp open  exec      syn-ack netkit-rsh rexecd  
513/tcp open  login     syn-ack  
514/tcp open  tcpwrapped syn-ack  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Rexec is very rarely present on modern networking environments due to numerous security weaknesses, such as a lack of

Rexec Service

```
512/tcp open  exec      syn-ack netkit-rsh rexecd  
513/tcp open  login     syn-ack  
514/tcp open  tcpwrapped syn-ack  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Rexec is very rarely present on modern networking environments due to numerous security weaknesses--

Privilege Escalation

Sudo Tmux

```
dfarrell@localhost:~/Projects
File Edit View Search Terminal Help

COMPUUPDATE ON;
end transaction;
DEBUG: Upload for hour 22 complete
DEBUG: Upload for hour 21 complete
DEBUG: Upload for hour 20 complete
DEBUG: Upload for hour 18 complete
DEBUG: Upload for hour 17 complete
DEBUG: Upload for hour 03 complete
DEBUG: Upload for hour 14 complete
DEBUG: Upload for hour 13 complete
DEBUG: Upload for hour 12 complete
DEBUG: Upload for hour 11 complete
DEBUG: Upload for hour 10 complete
DEBUG: Upload for hour 09 complete
DEBUG: Upload for hour 04 complete
DEBUG: Upload for hour 08 complete
DEBUG: Upload for hour 05 complete
DEBUG: Upload for hour 07 complete

DEBUG: Upload for hour 01 complete
DEBUG: Upload for hour 23 complete
DEBUG: Upload for hour 00 complete
DEBUG: Upload for hour 21 complete
DEBUG: Upload for hour 20 complete
DEBUG: Upload for hour 19 complete
DEBUG: Upload for hour 02 complete
DEBUG: Upload for hour 18 complete
DEBUG: Upload for hour 17 complete
DEBUG: Upload for hour 12 complete
DEBUG: Upload for hour 15 complete
DEBUG: Upload for hour 10 complete
DEBUG: Upload for hour 11 complete
DEBUG: Upload for hour 09 complete
DEBUG: Upload for hour 06 complete
DEBUG: Upload for hour 08 complete
DEBUG: Upload for hour 03 complete

from 's3://redshift.
ens_06.csv'
credentials 'aws_access_key_id=
s_key=
ACCEPTINVCHARS
format as CSV
IGNOREBLANKLINES DELIMITER ','
MAXERROR 0
DATEFORMAT 'auto'
TIMEFORMAT 'auto'
TRUNCATECOLUMNS
COMPUUPDATE ON;
end transaction;
DEBUG: uploading file to S3: /mnt/tmp/load_table_redshift.0h MFa/opens.0
8.csv => s3://redshift.
ns_08.csv
DEBUG: uploading file to S3: /mnt/tmp/load_table_redshift.CWh8RL/opens.0
7.csv => s3://redshift.
ns_07.csv

1 [||||100.0%] 9 [||||100.0%] 17 [||||100.0%] 25 [||||100.0%]
2 [||||100.0%] 10 [||||98.7%] 18 [||||97.4%] 26 [||||98.1%]
3 [||||100.0%] 11 [||||100.0%] 19 [||||100.0%] 27 [||||100.0%]
4 [||||100.0%] 12 [||||100.0%] 20 [||||100.0%] 28 [||||100.0%]
5 [||||100.0%] 13 [||||100.0%] 21 [||||100.0%] 29 [||||100.0%]
6 [||||100.0%] 14 [||||100.0%] 22 [||||100.0%] 30 [||||100.0%]
7 [||||100.0%] 15 [||||100.0%] 23 [||||100.0%] 31 [||||100.0%]
8 [||||100.0%] 16 [||||100.0%] 24 [||||100.0%] 32 [||||100.0%]
Mem [|||||||||56518/60140M] Tasks: 328, 17 thr; 209 running
Swp [|||||0/0MB] Load average: 137.52 44.35 16.99
Uptime: 00:51:19

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
7854 dfarrell 20 0 110M 757M 5744 R 100.0 1.3 1:14.00 perl /var
7859 dfarrell 20 0 1102M 748M 5744 R 99.0 1.2 1:14.62 perl /var
7861 dfarrell 20 0 1093M 739M 5744 R 99.0 1.2 1:14.98 perl /var
7858 dfarrell 20 0 1102M 749M 5744 R 99.0 1.2 1:12.87 perl /var
7856 dfarrell 20 0 1121M 768M 5744 R 94.0 1.3 1:14.68 perl /var

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice F8Nice F9Kill
```

Tmux is a terminal multiplexing program which allows users to split a single terminal window into multiple sections

Privilege Escalation

Sudo Tmux



```
sudo tmux
```

Since we have sudo access to the Tmux program, we can open a Tmux terminal with root access. We simply need use the command indicated above