Checked the auth.log for 172.16.0.21 (Dave) using “cat /var/log/auth.log”

* Unauthorized login from 172.16.0.32
* Can also use the command “lastlog” to view the last logins
* Below is the log from using “lastlog”

Username Port From Latest  
root pts/0 172.16.0.32 Wed Jan 16 15:42:55 -0800 2019  
daemon \*\*Never logged in\*\*  
bin \*\*Never logged in\*\*  
sys \*\*Never logged in\*\*  
sync \*\*Never logged in\*\*  
games \*\*Never logged in\*\*  
man \*\*Never logged in\*\*  
lp \*\*Never logged in\*\*  
mail \*\*Never logged in\*\*  
news \*\*Never logged in\*\*  
uucp \*\*Never logged in\*\*  
proxy \*\*Never logged in\*\*  
www-data \*\*Never logged in\*\*  
backup \*\*Never logged in\*\*  
list \*\*Never logged in\*\*  
irc \*\*Never logged in\*\*  
gnats \*\*Never logged in\*\*  
nobody \*\*Never logged in\*\*  
systemd-timesync \*\*Never logged in\*\*  
systemd-network \*\*Never logged in\*\*  
systemd-resolve \*\*Never logged in\*\*  
systemd-bus-proxy \*\*Never logged in\*\*  
messagebus \*\*Never logged in\*\*  
avahi \*\*Never logged in\*\*  
Debian-exim \*\*Never logged in\*\*  
statd \*\*Never logged in\*\*  
colord \*\*Never logged in\*\*  
geoclue \*\*Never logged in\*\*  
speech-dispatcher \*\*Never logged in\*\*  
sshd \*\*Never logged in\*\*  
pulse \*\*Never logged in\*\*  
rtkit \*\*Never logged in\*\*  
saned \*\*Never logged in\*\*  
usbmux \*\*Never logged in\*\*  
lightdm \*\*Never logged in\*\*  
hplip \*\*Never logged in\*\*  
administrator \*\*Never logged in\*\*  
vnc \*\*Never logged in\*\*  
telnetd \*\*Never logged in\*\*  
xrdp \*\*Never logged in\*\*  
proftpd \*\*Never logged in\*\*  
ftp \*\*Never logged in\*\*  
ntp \*\*Never logged in\*\*  
ashinkle \*\*Never logged in\*\*  
calabaster \*\*Never logged in\*\*  
erodriguez \*\*Never logged in\*\*  
rsimmons \*\*Never logged in\*\*  
abristille \*\*Never logged in\*\*  
hwilliams \*\*Never logged in\*\*  
mchen \*\*Never logged in\*\*  
mmitchell \*\*Never logged in\*\*  
nridgemont \*\*Never logged in\*\*  
dgrouper \*\*Never logged in\*\*  
splunk \*\*Never logged in\*\*

* To prevent this from happening again first we kill the telnet process and then go into “/etc/inetd.conf” and comment out the telnet line to disable the service.