Attack path:

Using dirsearch, I found the web link /dev/phpbash.php, which gives me a nonpersistent shell. What is going on with each command is that each command spawns a new shell. To get a persistent shell, we have to do a reverse shell. I saw that the /var/www/html/uploads folder had read, write, and execute permissions so I uploaded a reverse php shell. I used sudo -u scriptmanager bash to elevate my privileges and python -c ‘import pty; pty.spawn(“/bin/bash”)’ to create a fully functional shell. I then noticed that there was an unusual folder called scripts in the root directory. Looking at the test.py and test.txt file, I noticed that the dates are regularly updated meaning that the running of test.py is done by some scheduled process with root permissions. I replaced the test.py code with the python reverse shell code from http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet. I set up a listener on my machine to get the privileged shell after waiting around a minute.