**Enumeration**

Ill start by preforming an nmap scan on the box, the results…

Graphical user interface, text

Description automatically generated

Looks like there is a website and SSH running on this box. Searching the directories using Dirsearch. Results….

Text

Description automatically generated

**Foothold**

Going to the webpage brings us to a login screen. Viewing the source of the page shows that they are using Drupal 7.Text

Description automatically generated

A quick google search shows that Drupal 7 is vulnerable to attack. <https://www.rapid7.com/db/modules/exploit/unix/webapp/drupal_drupalgeddon2/>

After opening msfconsle we can use exploit/unix/webapp/drupal\_drupalgeddon2

Set our RHOST, LHOST, and targetID and exploit.

Text

Description automatically generated

We have now gained access to the box.

Looking in the directory we can access the sites/default folders to get to settings.php.

Text

Description automatically generated

Cat these settings out to find the mysql database user id and password.

drupaluser: CQHEy@9M\*m23gBVj

mysql -u drupaluser -p -D drupal -e ‘show tables;’

enter password CQHEy@9M\*m23gBVj

Text

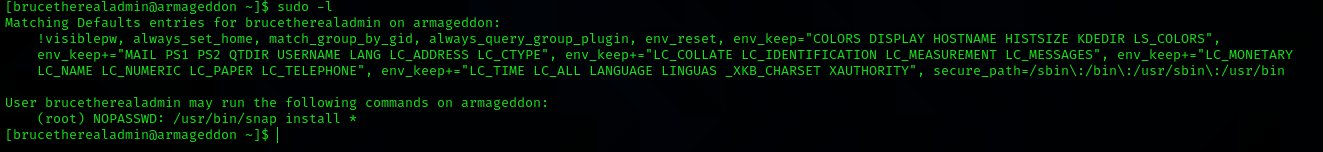
Description automatically generated

Now to run the hashes through John the ripper.

After cracking the password, ssh into the box to gain user.txt

Brucetherealadmin:booboo

Sudo -l to check permissions



<https://github.com/initstring/dirty_sock/blob/master/dirty_sockv2.py>

python -c 'print "" + "A"\*4256 + "=="' | base64 -d > root.snap

sudo /usr/bin/snap install - devmode meet.snap