# *OpenAdmin (Linux)*

Some new things I learned/used for the first time with this challenge:

**Enumeration**:

Nothing too complex at all here. Just nmap finds a web server running, ffuf finds some directories, the directory leads me to an OpenAdmin page that gives me the version along with it.
This version of OpenAdmin was vulnerable to an unauthenticated remote code execution.

https://www.exploit-db.com/exploits/47691

The PoC is the github I thought was a little better then what was on exploit-db
https://github.com/amriunix/ona-rce

**Foothold:**
Once we have our shell we can see that we are the www-data user. Run linpeas tells us there is a webserver running locally on some ephermal port.
From linpeas we can also enumerate that there are two users on the system, "jimmy" and "joanna". The "joanna" user has some sudo priviliges but I can't view what they are.
Whenever there are multiple users, that almost gurantees there will be some lateral movement involved.

As www-data, this user is, usually, able to read database configuration files. It is always smart to check for password re-use.
I was able to find a password for the jimmy user by looking through the web server's config files.

I mentioned earlier that linpeas revealed a local port open for an internal webserver.
With this jimmy user we can now view what is inside of the internal webserver's web directories.
Inside of the web directory is a hard coded sha256 password hash that can be cracked to be used for this internal web server.

Once you do some local port forwarding via ssh like so

```
ssh jimmy@10.129.95.149 -L 52846:127.0.0.1:52846
```

You will now be able to access that internal web server from your browser when you visit the localhost address.
Using the credentials that we cracked leads us to a page that contains an ssh private key.

With this private key we can use a tool called **ssh2john** to pull a hash from that ssh priv key.
Then run rockyou on the wordlist to find the final credentials we need to access that "joanna" user.

**Priv Esc**
As I mentioned before, linpeas discovered that this "joanna" user that I am now logged in as, has some sudo permissions.

Doing sudo -l reveals that we are allowed to run nano as root. Then us gtfobins to find out that you can execute a command while inside of nano with some keyboard shortcuts. Then you have root :)

This was a fun box!