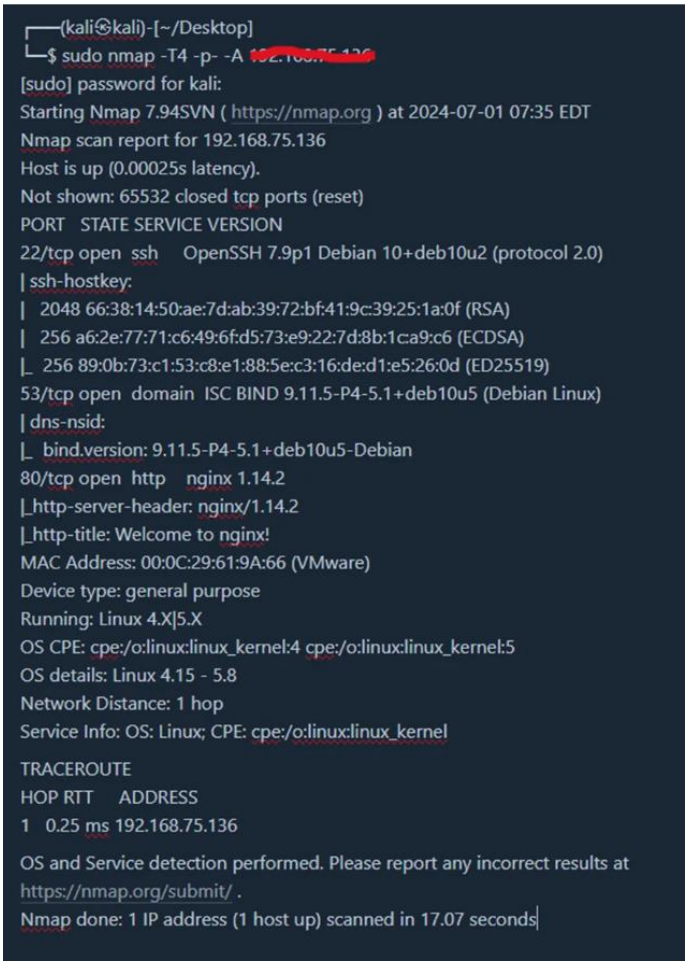
Blackpearl box walkthrough, this is a test to see what I am missing in future report writing. This is written as a walkthrough and at the end I plan on writing notes critiquing myself as to what I am missing from my notes to improve my methodology and improve my report writing in anticipation of my PNPT exam.

Findings for blackpearl a capstone machine from TCM Security's Practical Ethical Hacker course, this is where I start to fumble with creating my own checklist and methodology and learning proper methodology and fix bad habits I currently have.

First things first, nmap scan, I used the following command to get a nmap scan for the box.

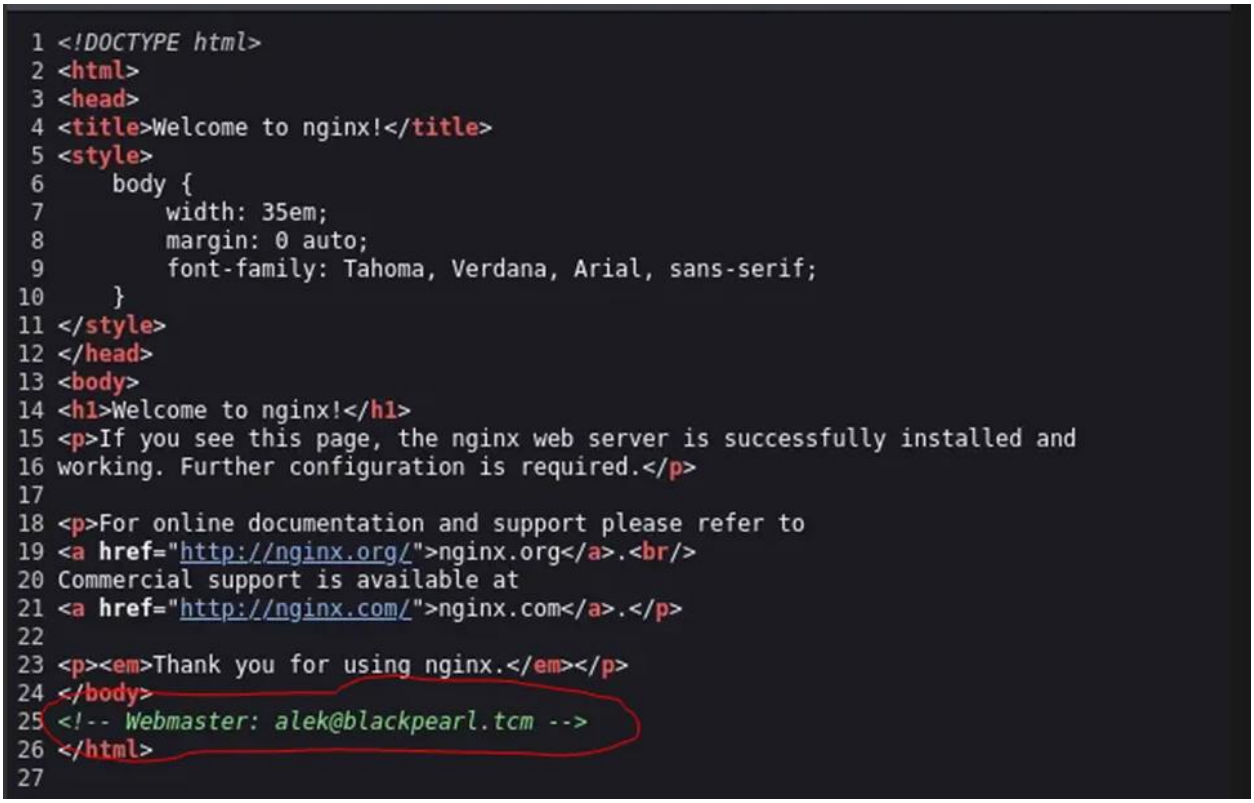
```
sudo nmap -T4 -p- -A <IP>
```



We have 3 ports that come back with a possible OS for the blackpearl box. Currently the belief is that Blackpearl is a Linux based system, running nginx http server, OpenSSH for

external connections and port 53 which is DNS. We can get this information from the NMAP scan, now we can start going after the easy wins for enumeration. Port 80.

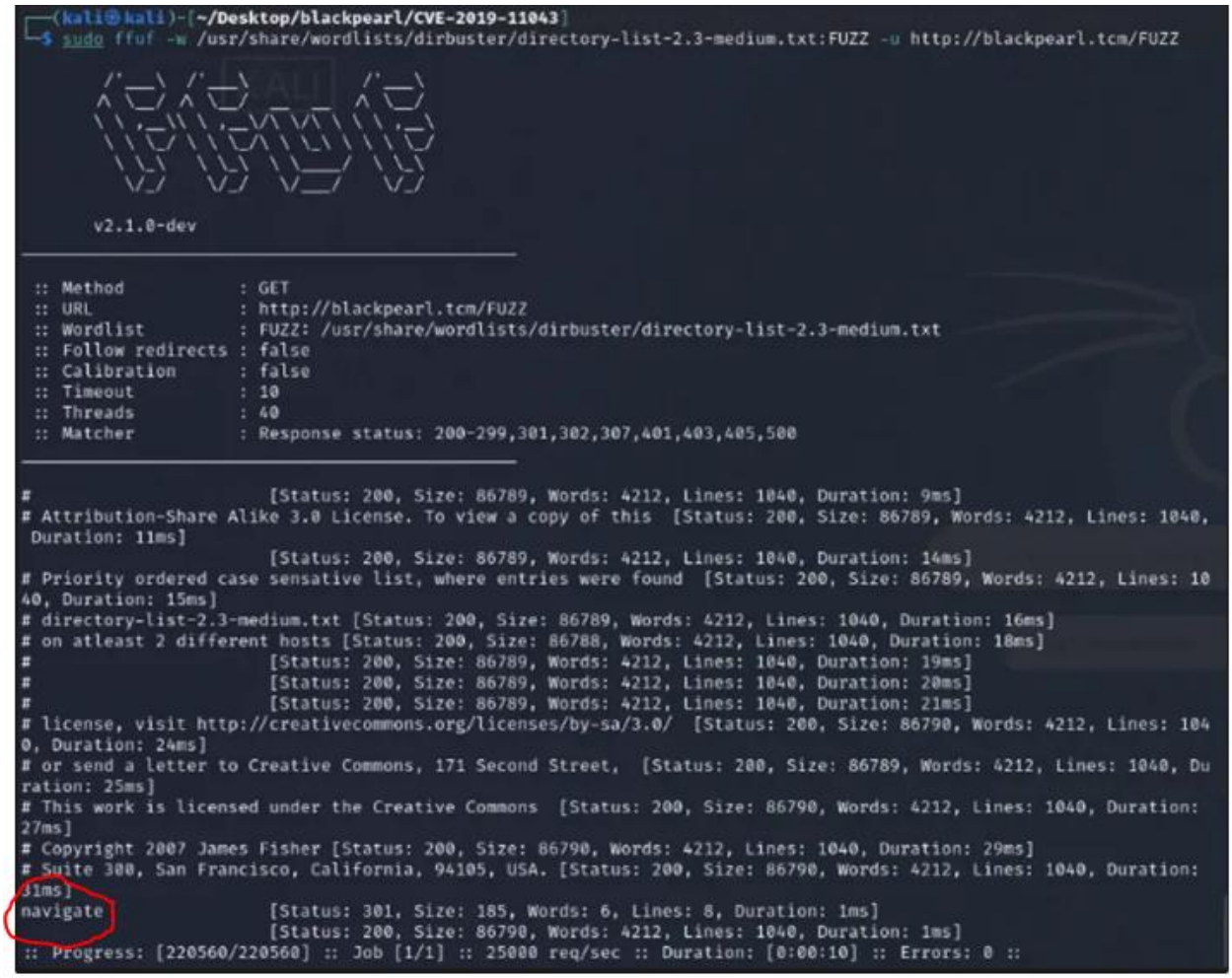
The webpage itself is a default webpage, however if we go to the read me source, then we can collect the possible domain name for the system from a comment from the webmaster.



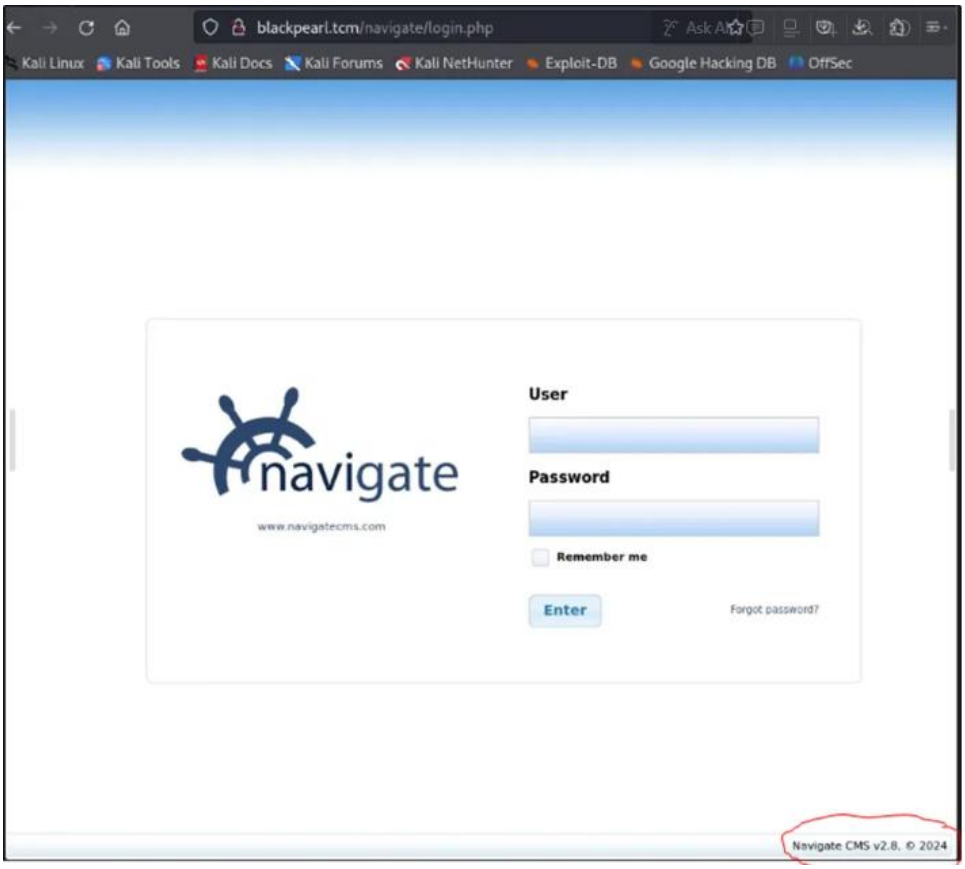
```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
<!-- Webmaster: alek@blackpearl.tcm -->
</html>

```

If we further enumerate and start directory busting using FFUF, we can see there is a navigate directory.

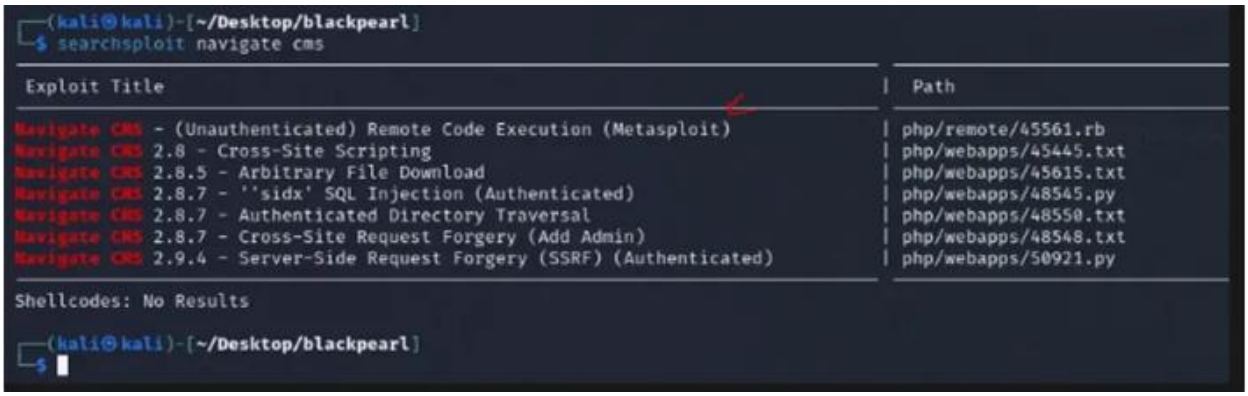
```
sudo ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u <http://ip/FUZZ>
```



Then starting the first attempt try to directory bust using FFUF, using the IP address rather than the domain of *blackpearl.tcm*.

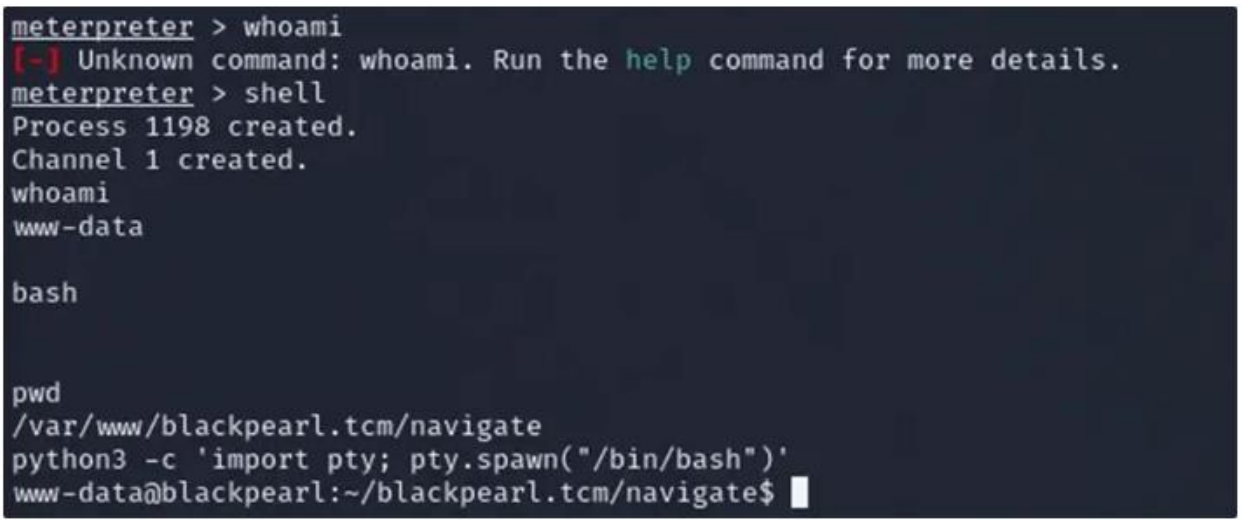


Once we navigate to blackpearl.tcm/navigate we have a login page that pops up, which is running CMSv2.8. Now lets look for exploits, I like to look up via searchsploit first, then go to the internet because if I can find it via searchsploit it saves time and fighting with google to get the same exploit. You will see that Metasploit has a module for navigate cms that we can use, for Unauthenticated Remote Code Execution.



After setting up all of the options and the ports to run this exploit, I dropped into a shell as www-data user and attempted to make the meterpreter shell more stable by using import pty.

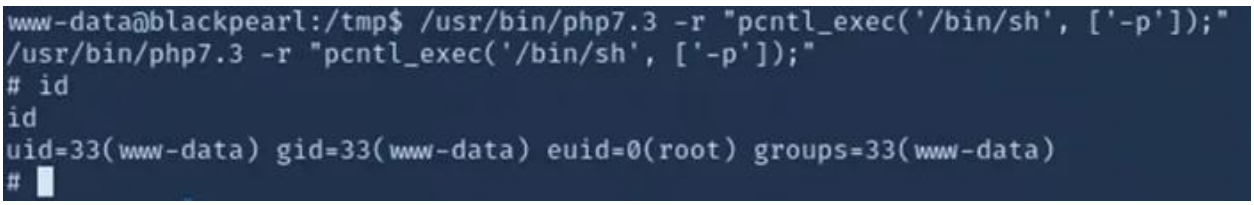
`python3 –c ‘import pty;pty.spawn(“/bin/bash”)’`



Once you have a meterpreter shell you can hunt for some easy wins, the first one that I did was searching for SUID and SGID that I could look up for root access. The command I used for this enumeration is:

```
find / -type f -perm -4000 2>/dev/null
```

Found a vulnerability for php7.3 from GTFObins which allows for a root shell.



I am now root neat!

Things to improve:

More Pictures

See if I can inverse the photos to save on ink for prospective customer.