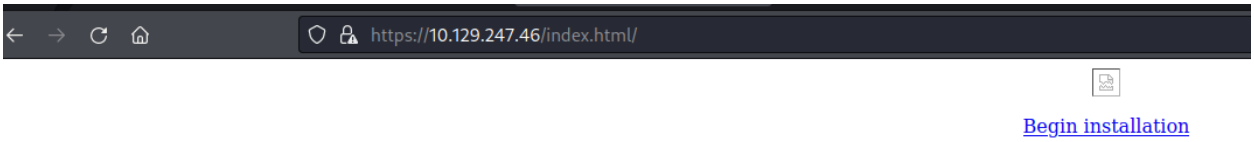
Sense –

As the first step, used **Nmap** tool to scan for open ports and services on the machine.

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     lighttpd 1.4.35
|_http-title: Did not follow redirect to https://10.129.247.46/
|_http-server-header: lighttpd/1.4.35
443/tcp open  ssl/http lighttpd 1.4.35
|_http-title: Login
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName
| Not valid before: 2017-10-14T19:21:35
|_Not valid after:  2023-04-06T19:21:35
|_ssl-date: TLS randomness does not represent time
|_http-server-header: lighttpd/1.4.35
```

With only port 80 & 443 open on the machine, used **Gobuster** to enumerate the sub-directories of the website.

```
/classes              (Status: 301) [Size: 0] [--> https://10.129.247.46/classes/]
/css                  (Status: 301) [Size: 0] [--> https://10.129.247.46/css/]
/favicon.ico          (Status: 200) [Size: 1406]
/includes             (Status: 301) [Size: 0] [--> https://10.129.247.46/includes/]
/index.html           (Status: 200) [Size: 329]
/index.php            (Status: 200) [Size: 6690]
/installer            (Status: 301) [Size: 0] [--> https://10.129.247.46/installer/]
/javascript           (Status: 301) [Size: 0] [--> https://10.129.247.46/javascript/]
/themes               (Status: 301) [Size: 0] [--> https://10.129.247.46/themes/]
/tree                 (Status: 301) [Size: 0] [--> https://10.129.247.46/tree/]
/widgets              (Status: 301) [Size: 0] [--> https://10.129.247.46/widgets/]
/xmlrpc.php           (Status: 200) [Size: 384]
```



Open checking one of the subdirector's source code, it shows some information on SSH service but the port 22 is closed when scanned using **Nmap.**

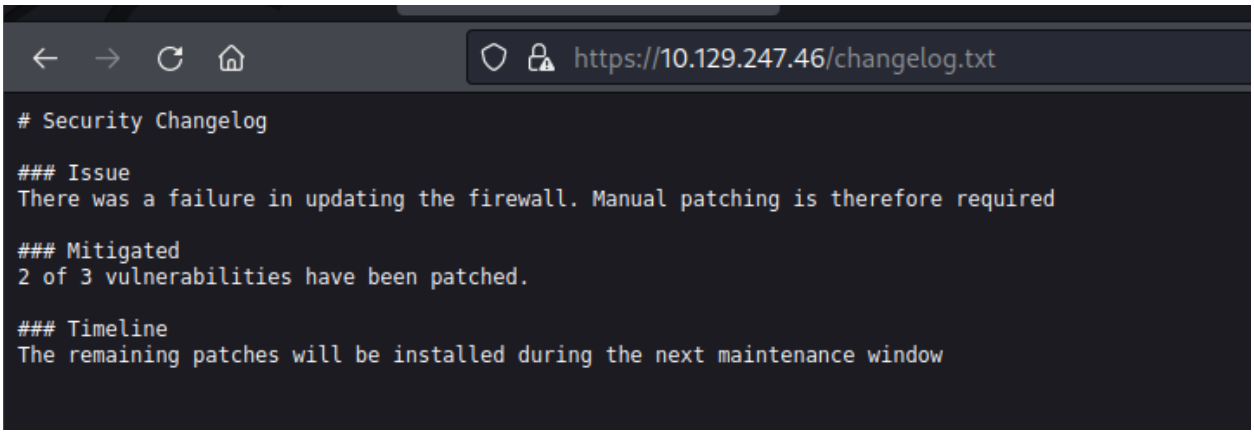
```
</p>

<!--
<p>
    Connect to host via SSH:
    <applet CODEBASE="." ARCHIVE="jta20.jar" CODE="de.mud.jta.Applet" WIDTH=55 HEIGHT=25>
    <param NAME="config" VALUE="applet.conf">
    </applet>
</p>
-->

</center>
```

Since we didn't get much information from the above Gobuster results, now scanned with more appropriate wordlist with txt,html and php extensions.

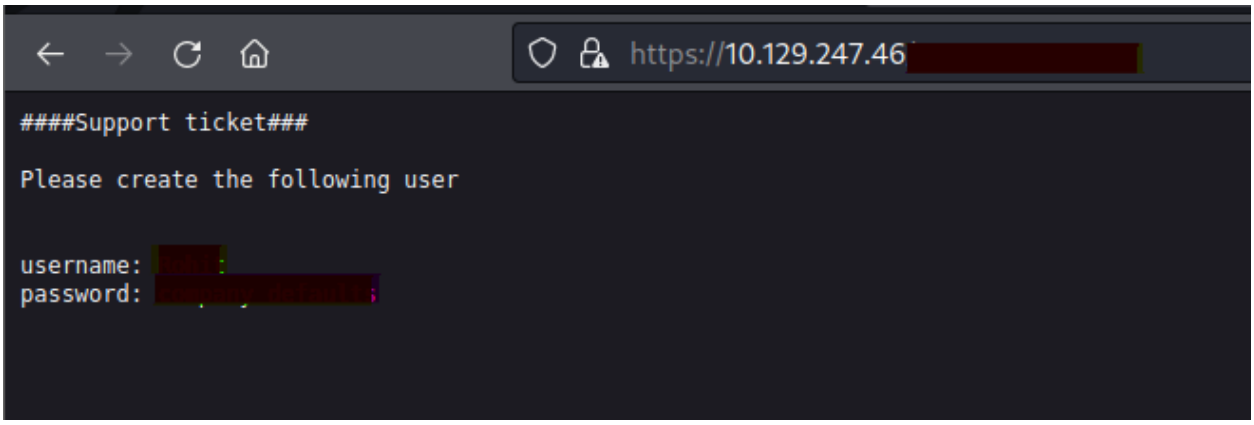
```
/index.html           (Status: 200) [Size: 329]
/index.php            (Status: 200) [Size: 6690]
/help.php             (Status: 200) [Size: 6689]
/themes               (Status: 301) [Size: 0] [--> https://10.129.247.46/themes/]
/stats.php            (Status: 200) [Size: 6690]
/css                  (Status: 301) [Size: 0] [--> https://10.129.247.46/css/]
/edit.php             (Status: 200) [Size: 6689]
/includes             (Status: 301) [Size: 0] [--> https://10.129.247.46/includes/]
/license.php          (Status: 200) [Size: 6692]
/system.php           (Status: 200) [Size: 6691]
/status.php           (Status: 200) [Size: 6691]
/javascript           (Status: 301) [Size: 0] [--> https://10.129.247.46/javascript/]
/changelog.txt        (Status: 200) [Size: 271]
/classes              (Status: 301) [Size: 0] [--> https://10.129.247.46/classes/]
/exec.php             (Status: 200) [Size: 6689]
/widgets              (Status: 301) [Size: 0] [--> https://10.129.247.46/widgets/]
/graph.php            (Status: 200) [Size: 6690]
/tree                 (Status: 301) [Size: 0] [--> https://10.129.247.46/tree/]
/wizard.php           (Status: 200) [Size: 6691]
/shortcuts            (Status: 301) [Size: 0] [--> https://10.129.247.46/shortcuts/]
/pkg.php              (Status: 200) [Size: 6688]
/installer            (Status: 301) [Size: 0] [--> https://10.129.247.46/installer/]
/wizards              (Status: 301) [Size: 0] [--> https://10.129.247.46/wizards/]
/xmlrpc.php           (Status: 200) [Size: 384]
/reboot.php           (Status: 200) [Size: 6691]
/interfaces.php       (Status: 200) [Size: 6695]
/csrf                 (Status: 301) [Size: 0] [--> https://10.129.247.46/csrf/]
/system-users.txt     (Status: 200) [Size: 106]
/filebrowser          (Status: 301) [Size: 0] [--> https://10.129.247.46/filebrowser/]
/%7echeckout%7e       (Status: 403) [Size: 345]
```

The above scan results revealed us with more sub-directories – **changelog.txt and system-users.txt** files.

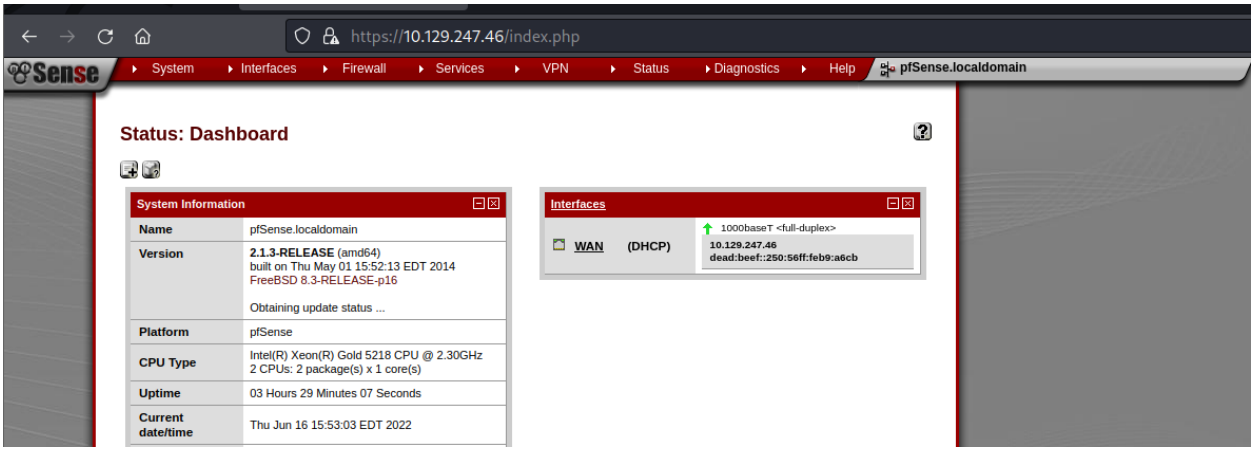
The change-log.txt file shows that 2 of the 3 vulnerabilities have been fixed. Hence we need to find and exploit the 3rd vulnerability which hasn't been fixed yet.



Another sub-directory reveals us with the credentials for logging into the PFsense portal which is hosted on the server.

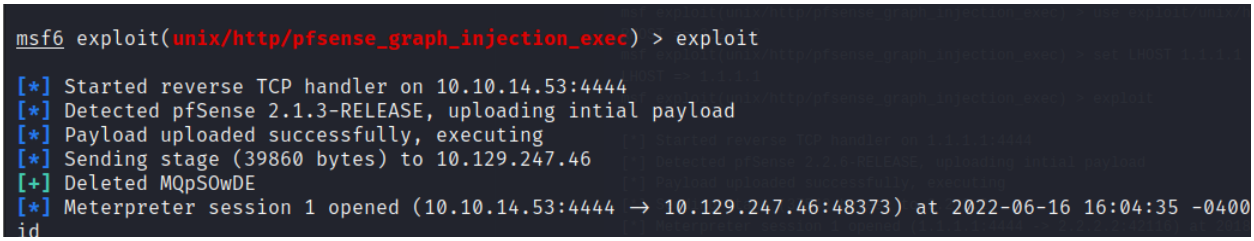


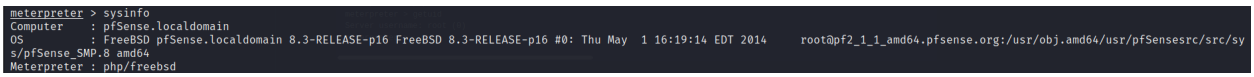
Successfully logged in to the Pfsesnse portal!



As researched more on the exploits of the version of PfSense installed which is v2.1.3-RELEASE(amd64), we found a article which explains the ways to exploit the same – (https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/unix/http/pfsense_graph_injection_exec.md)

Follow the article to use Metasploit to exploit the machine further.





The exploit provides us with root access to the machine and we get access to the root flag and hence owned the machine.