Sense –

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

Text

Description automatically generated

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

A picture containing text

Description automatically generated

Graphical user interface, application

Description automatically generated

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.**

A picture containing text

Description automatically generated

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

A computer screen capture

Description automatically generated with medium confidence

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.

A screenshot of a computer screen

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

Successfully logged in to the Pfsesnse portal!

Graphical user interface

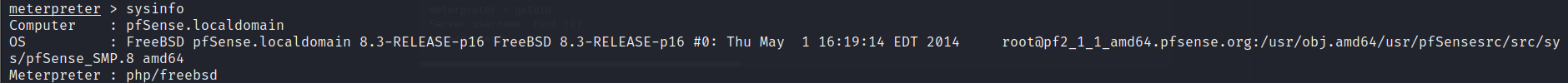
Description automatically generated

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.

Graphical user interface, text

Description automatically generated



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

Text

Description automatically generated with low confidence