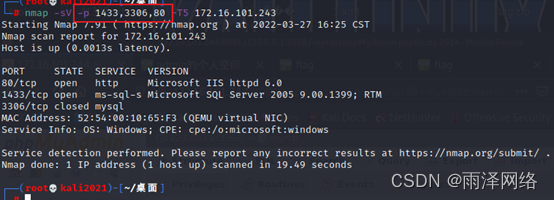
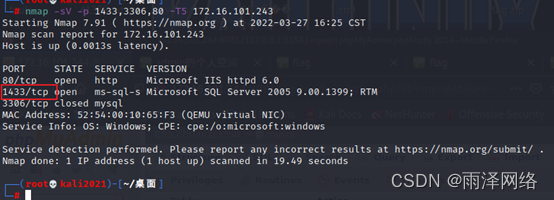
**B-1任务一：数据库**[渗透](https://so.csdn.net/so/search?q=%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95&spm=1001.2101.3001.7020)

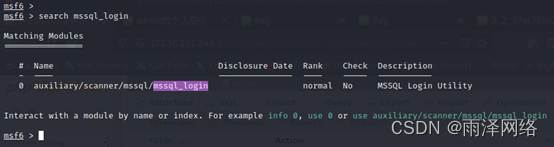
1. 在渗透机Kali2.0中使用zenmap工具扫描服务器场景Server2所在[网段](https://so.csdn.net/so/search?q=%E7%BD%91%E6%AE%B5&spm=1001.2101.3001.7020)(例如：172.16.101.0/24)范围内存活的主机IP地址和指定开放的1433、3306、80端口。并将该操作使用的命令中必须要使用的字符串作为Flag值提交；



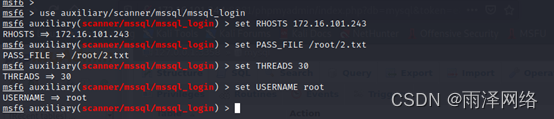
1. 通过渗透机Kali2.0对服务器场景Server2进行系统服务及版本扫描渗透测试，并将该操作显示结果中数据库服务对应的服务端口信息作为Flag值提交；



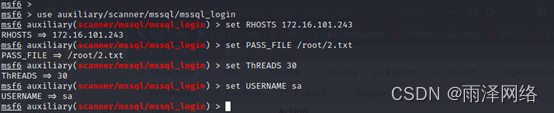
3.在渗透机Kali2.0中使用MSF中模块对其爆破，使用search命令，并将扫描弱口令模块的名称作为Flag值提交；



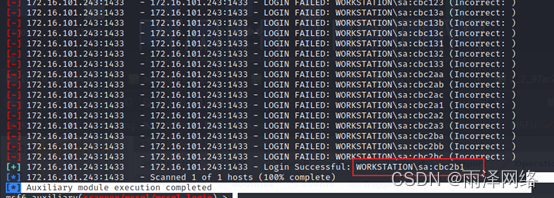
1. 在上一题的基础上使用命令调用该模块，并查看需要配置的信息（使用show options命令），将回显中需要配置的目标地址,密码使用的猜解字典,线程,账户配置参数的字段作为Flag值（之间以英文逗号分隔，例hello,test，..,..）提交；



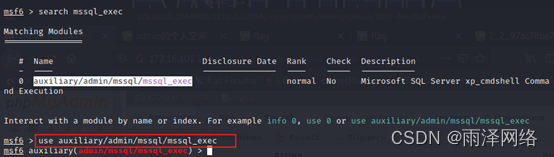
1. 在msf模块中配置目标靶机IP地址，将配置命令中的前两个单词作为Flag值提交；



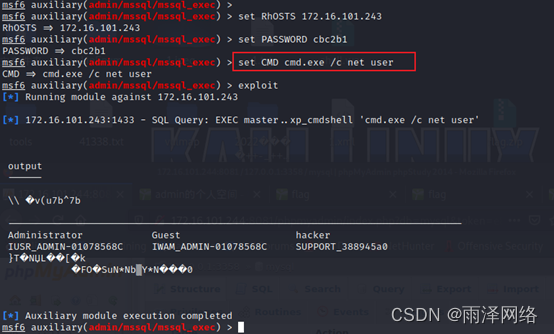
6.在msf模块中指定密码字典，字典路径为/root/2.txt爆破获取密码并将得到的密码作为Flag值提交；



7.在msf模块中切换新的渗透模块，对服务器场景server2003进行数据库服务扩展存储过程进行利用，将调用该模块的命令作为Flag值提交；



8.在上一题的基础上，使用第6题获取到的密码并进行提权，同时使用show options命令查看需要的配置，并配置CMD参数来查看系统用户，将配置的命令作为Flag值提交；



**B-2任务二：数据库安全加固**

\*任务说明：仅能获取Server6的IP地址

1.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），查看数据库版本号，将查看数据库版本号的命令作为Flag值提交；

Flag:select version();



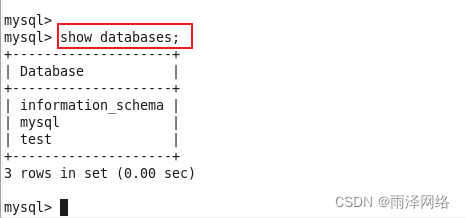
2.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），查看数据库版本号，将查询到的数据库版本号作为Flag值提交；

Flag：5.1.73



3.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），查看数据库列表，将查看数据库列表的命令作为Flag值提交；

Flag:show databases;



4.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），进入MySQL数据库，查看所有用户及权限，找到可以从任意 IP 地址访问的用户，将该用户的用户名作为Flag值提交；（如有多个可以从任意 IP 地址访问的用户，提交形式为用户名|用户名|用户名|用户名）

Flag:test



5.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），进入MySQL数据库，查看所有用户及权限，找到可以从任意 IP 地址访问的用户，使用drop命令将该用户删除，将操作命令作为Flag值提交；

Flag: drop user ‘test’@’%’;



6.进入虚拟机操作系统：CentOS 6.8，登陆数据库（用户名：root；密码：root），进入MySQL数据库，改变默认 MySQL 管理员的名称，将系统的默认管理员root 改为 admin，防止被列举，将操作命令作为Flag值提交。

Flag：update user set user=’admin’ where user=’root’;

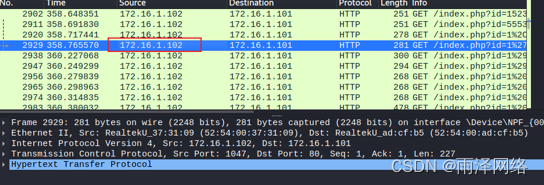


**B-2任务二：数据分析数字取证**

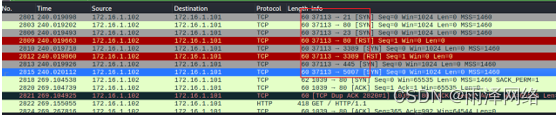
\*任务说明：仅能获取Server2的IP地址

1.使用Wireshark查看并分析Server2桌面下的attack.pcapng数据包文件，通过分析数据包attack.pcapng找出恶意用户的IP地址，并将恶意用户的IP地址作为Flag值（形式：[IP地址]）提交；

Flag：[172.16.1.102]

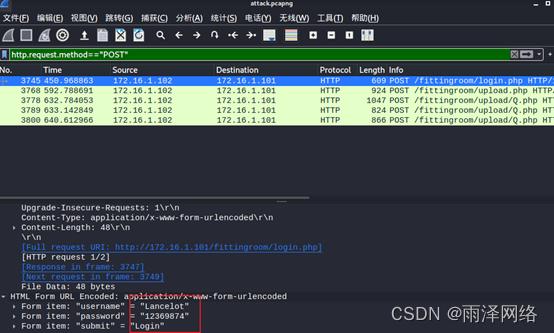


2.继续查看数据包文件attack.pacapng，分析出恶意用户扫描了哪些端口，并将全部的端口号从低到高作为Flag值（形式：[端口名1，端口名2，端口名3…，端口名n]）提交；



3.继续查看数据包文件attack.pacapng分析出恶意用户最终获得的用户名是什么，并将用户名作为Flag值（形式：[用户名]）提交；

Flag:[Lancelot]



4.继续查看数据包文件attack.pacapng分析出恶意用户最终获得的密码是什么，并将密码作为Flag值（形式：[密码]）提交；

见上一题

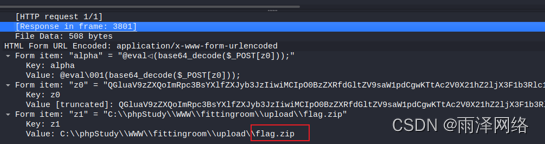
5.继续查看数据包文件attack.pacapng分析出恶意用户连接一句话木马的密码是什么，并将一句话密码作为Flag值（形式：[一句话密码]）提交；

Flag:[alpha]



6.继续查看数据包文件attack.pacapng分析出恶意用户下载了什么文件，并将文件名及后缀作为Flag值（形式：[文件名.后缀名]）提交；

[flag.zip]



7.继续查看数据包文件attack.pacapng将恶意用户下载的文件里面的内容作为Flag值（形式：[文件内容]）提交。

