**2023年信息安全工程师下午题（部分解析）**

**试题一：（15分）**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 15 | 1 | 8 | 14 | 6 | 11 | (1) | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 1 | 3 | (2) | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 2 | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | (3) | 8 | 12 | 6 | 9 | 3 | 2 | 5 |
| 3 | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | (4) | 5 | 14 | 9 |

1、已知 DES 算法S盒如下，请补全S盒空缺的数据(1)(2)(3)(4) (4分)

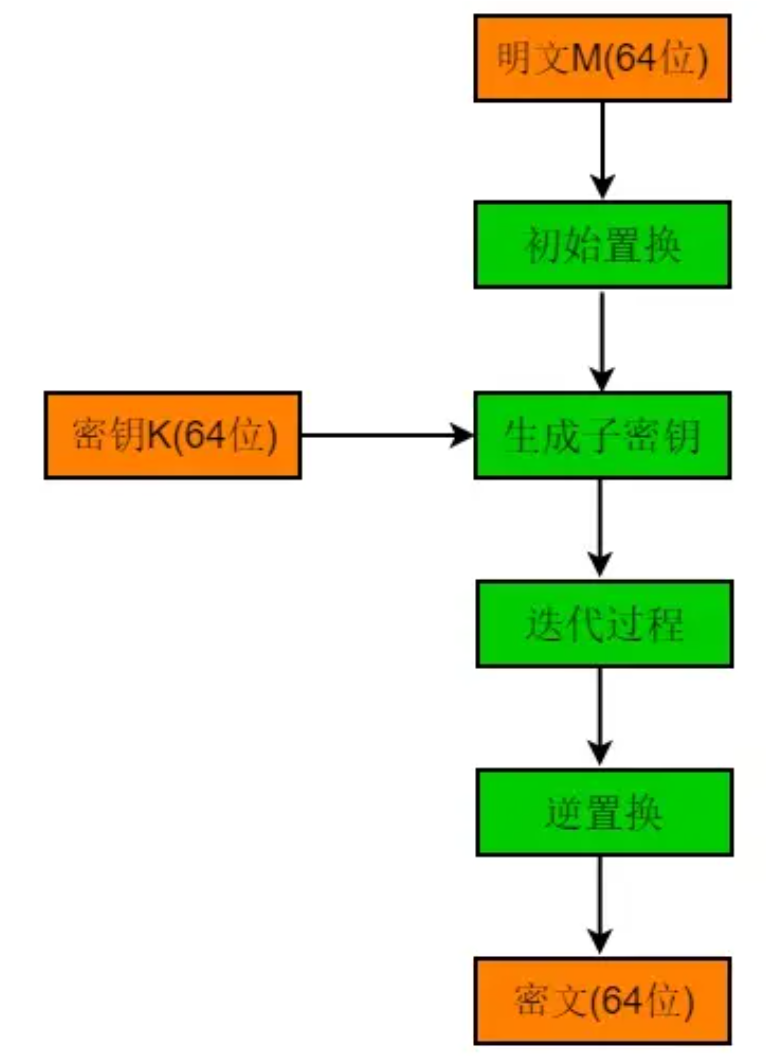
2、已知S盒的输入为 110011，请计算经过S盒变换之后的二进制输出。(2分)

3、使用 DES 算法对明文字符串“12345”进行加密，应当对明文进行填充，请问填充后的数据长度多少比特(位)?并给出填充后明文字符串表示。(3分)

4、如果使用密钥“\x01\x01\01\x01\x01W01\W01\x01”对明文进行加密，会出现什么安全问题?(2分)

5、不论古典密码还是现代密码，其中最为核心的操作是替代和置换，对应于香农的《保密系统的通信理论》论文中，分别对应哪两种密码技术?(2分)

6、在 DES 算法中，置换对应下图当中哪个操作部件?(2分)



**试题一参考答案及解析:**

1、参考答索:3、13、15、0

试题解析:S盒每一行的数字从0到15乱序排列，依次查看每一行哪一个数字没有，空格就应该填什么数字。

2、参考答案:0110

试题解析:输入为110011，取第一位和第六位为，转化为十选制3，中间四位为1001，转化为十进制9。在S盒中查看第3行第9列的数字为6，转换为二进制位0110。

3、64位、12345\x03\x03\x03

试题解析:DES 其法的明文分组长度为64位;字符串“12345”，ASCII 编码下每个字符占 8 比特，一共 5个字符，即40比特。所以需要填充24比特。一般采用 PKCSH5或PKCS#7 填充方式，这里假设采用PKCS#7 填充。在这个题目中需要填充3个字节，填充的值为3，用十六进制表示为03、03、03。所以填充后的明文字符串 ASCII编码表示为“12345\x03\x03\x03”。

4、参考答案:密钥重复，容易被破解。

试题解析:这个密钥非常简单且具有规律性，只有八个字节的值均为 0x0l。对于攻击者来说。通过分析加密数据的模式或者使用暴力破解方法，很容易尝试出这个密钥。

5、参考答索:混乱、扩散

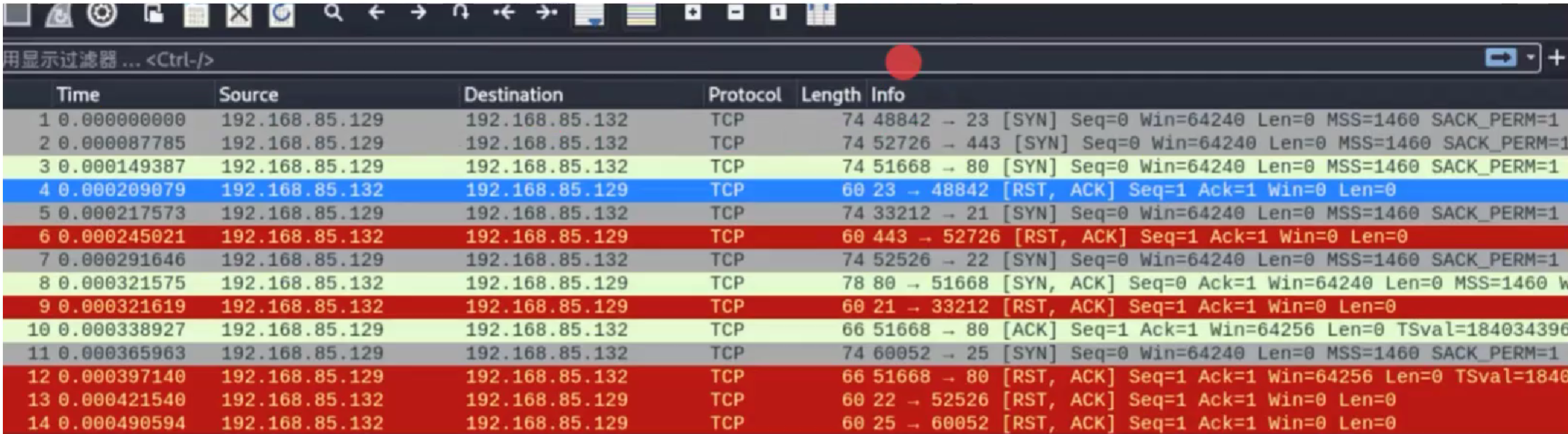
试题解析:在香农的《保密系统的通信理论》论文中，替代对应混乱技术，置换对应扩散技术。混乱使得密文与密钥的关系变得复杂，让攻击者难以从密文中推断出关于密钥的信息。替代操作实现了这种混乱处果。扩散将明文的统计特性扩散到整个密文中，使得明文的一个小变化会引起密文的很大变化。置换操作实现了这种扩散效果。

6、参考答案:初始置换、逆置换

试题解析:DES 算法通过初始置换将明文数据打乱，在每一轮的运算过程中也包含各种置换操作来改变数据的位置和分布，以实现扩散效果，增加密码的安全性。逆初始置换则在最后将密文数据恢复到一定的顺序以便输出。

**试题二（15分）**

Wireshark抓包信息如下：



1、根据 wireshark 流量包写出扫描源地址?(2分)

2、要产生如图流量包视图，请写出wireshark过滤规则?(2分)

3、根据流量包分析目标系统开放了哪些端口，说明理由?(3分)

4、此流量包属于什么类型扫描?(2分)

5、wireshark抓包截图中有很多RST/ACK分组，写出RST/ACK分组的tcp标志位值是多少?(2分)

6、如果要用iptables对这些扫描流量进行过滤，需要使用iptables fter表中哪条链?(2分)

7、写出一条 iptables 基于源地址防止以上扫描的过滤规则。(2分)

**试题二参考答案及解析:**

1、参考答案:192.168.85.129

试题解析:从图中 source 源地址以及源端口可以看出，源地址192.168.85.129对目标地址 192.168.85.132进行扫描。

2、参考答案:ip.src-192.168.85.129&&&ip.dst=192.168.85.132

试题解析:Wireshark 是一款强大的网络数据包分析工具，以下是一些基本的过滤规则介绍:一、基于协议过滤

过滤特定协议的数据包，例如:

http:只显示 HTP 协议的数据包。

tcp:显示T 协议的数据包。

udp:显示 UDP 协议的数据包。

二、基于 IP 地址过滤

源 IP 地址过滤:

ip.src==192.168.1.100:显示源IP地址为192.168.1.100 的数据包。目的 IP 地址过滤:

ip.dst==192.168.1.200:显示目的P地址为192.168.1.200的数摇包。

同时过滤源和目的 IP 地址:

ipsrc==192.168,1.100&&ipdst==192.168,1.200:显示源IP为192.168.1.100且目的IP192.168.1.200 的数据包。

三、基于端口过滤

源端口过滤:

tcp.srcport==80:显示TCP协议中源端口为80的数据包。

目的端口过滤:

tcp.dstport==8080:显示TP协议中目的端口为8080的数据包。

四、基于数据包内容过滤

过滤包含特定字符串的数据包:

http contains"login”:显示 HITTP数据包中包含“login”字符串的数据包。

五、基于数据包长度过滤

例如:frame.len>100:显示领长度大于100的数据包。

六、逻样运算符组合过滤

可以使用逻辑运算符如“and”(在 Wireshark 中通常用 “&&” 表示)、“or”(“|| ”)和“not”(“!”)未组会多个过滤条件。

例如:tcpport=80&&ip.src==192.168.1.100，表示显示源IP地址为192.168.1.100且使用 TCP端口 80 的数据包。

3、参考答案:80

试题解析:从抓包情况来看，只有80端口建立了完整的三次握手过程。

4、参考答案:完全连接扫描

试题解析:完全连接扫描利用 TCP/IP 协议的三次握手连接机制，使源主机和目的主机的某个端口建立一次完整的连接。如果建立成功，则表明该端口开放。否则，表明该端口关闭。

5、参考答案:0x14(二进制表示为 00010100)

试题解析:在 TCP协议中，RST(复位)和ACK(确认)是TCP报文的两个特殊标志位。在 TCP报文中，一个同时设置了 RST和 ACK 标志位的 TCP 报文的标志住值从左到右的顺序是:CWR:0,ECE:0,URG:0,ACK:1，PSH:0,RST:1，SYN:0，FIN:0这意味着这个 TCP 报文的标志位值是00010100，转化为16进制为0x14。

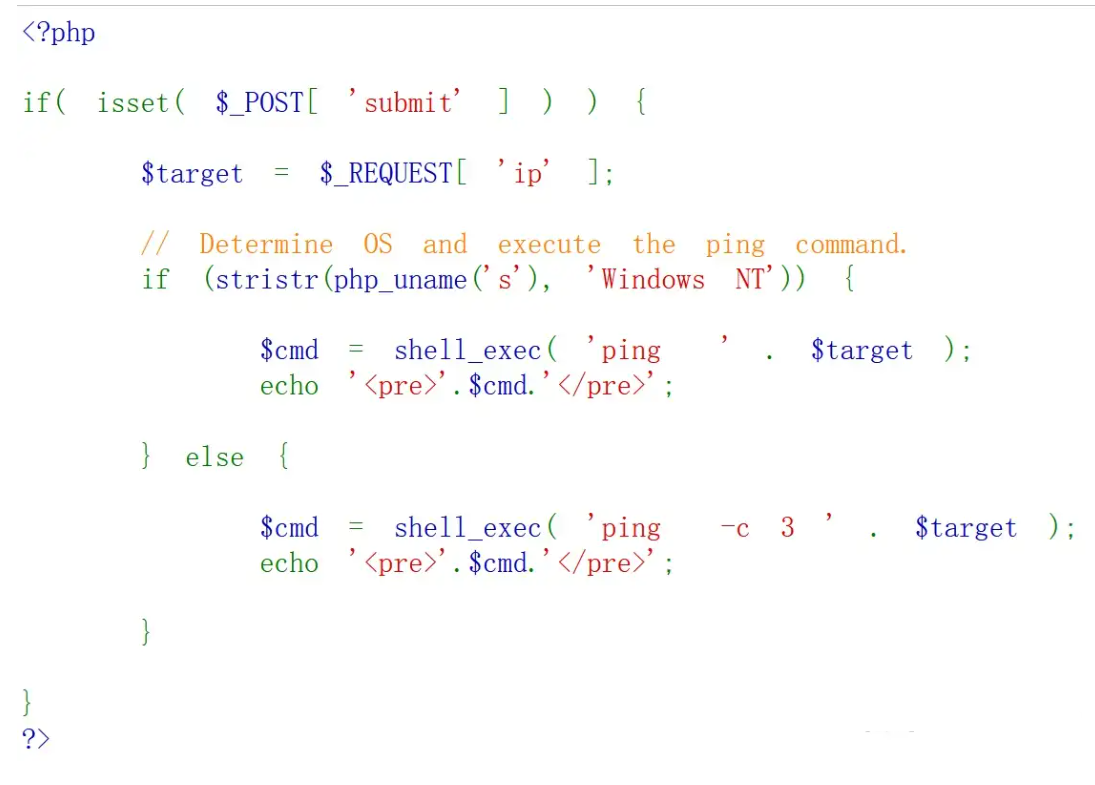
6、参考答案:INPUT 链。

试题解析:如果是在被扫描的主机上进行 iptables的配置，很明显是阻止从外到内的扫描流量，所以是 INPUT链。因为没有官方题目，题意可能不准确。姑且认为是在被扫描主机上配置。如果在扫描主机和被扫描主机之间有一个主机安装iptables作为防火墙使用，则为FORWARD链。

7、参考答案:iptables-AINPUT-s192,168,85.129-d192.168.85.132p tcp -J DROP或者iptables-AINPUT-s192.168.85.129-j DROP

试题解析:针对iptables的配置，案例课程有专门讲课。Iptables的配置规则必须要学会。

**试题三（15分）**



1.此代码存在什么漏洞？（2分）

2.客户端的HTTP请求类型是什么？（2分）

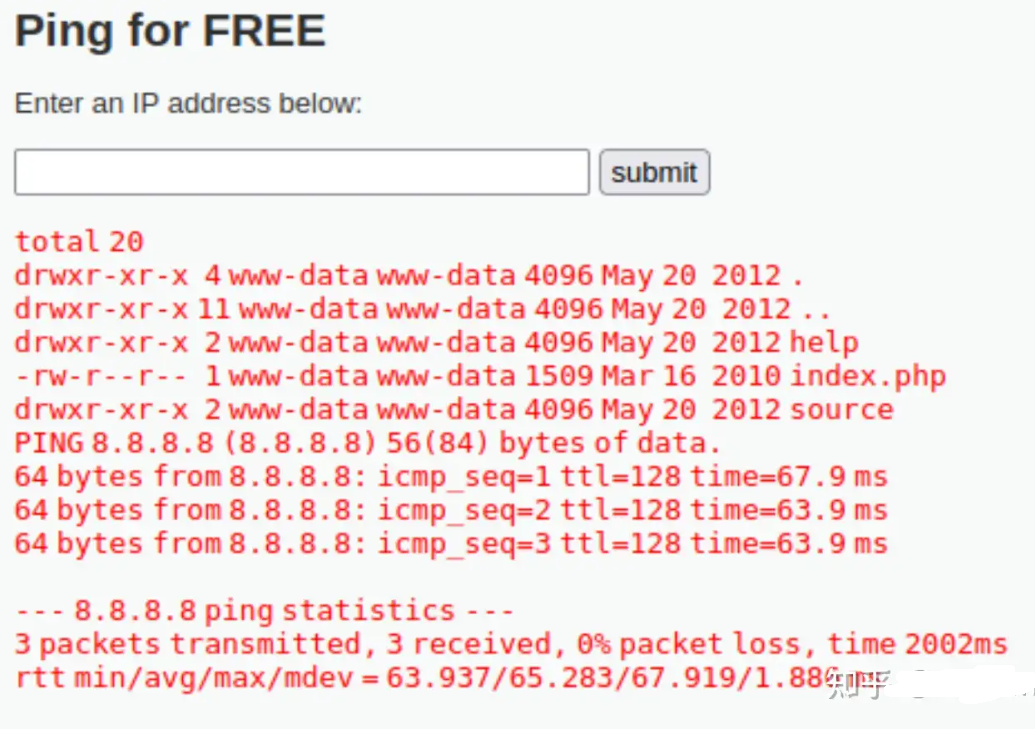
3.有几个参数，哪个参数会造成漏洞影响？（3分）

4.输入8.8.8.8，服务端执行什么命令？（2分）



5.使用content-type为multipart/form-data提交表单？（2分）

6. （4分）（1）输入什么命令，能输出如图的结果？



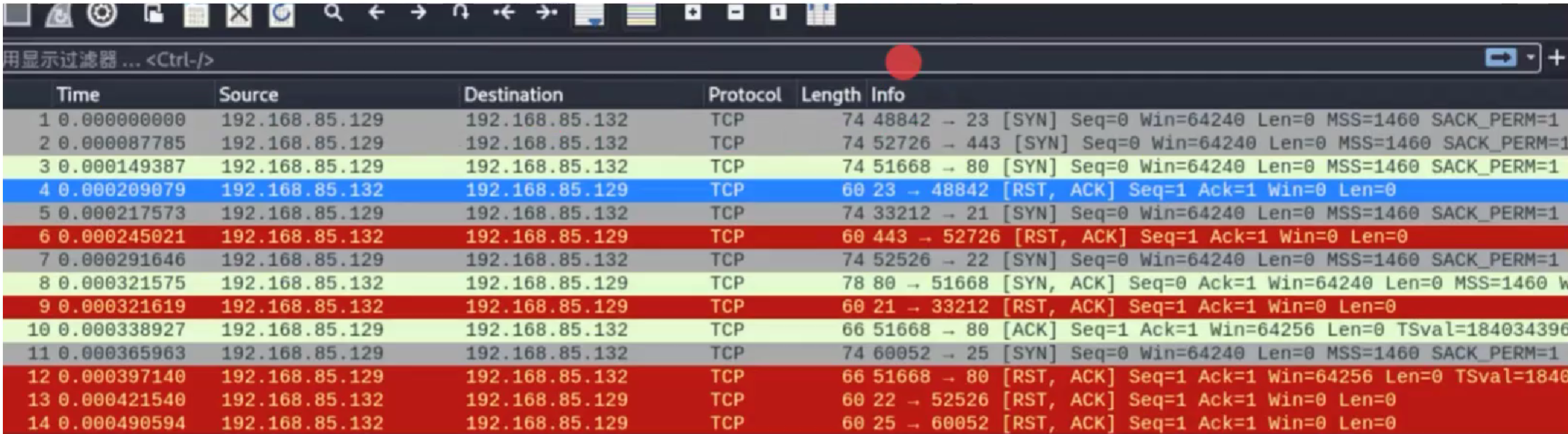
（2）www-data

【解说/吐槽】 1.命令执行/注入漏洞 2.POST请求 3. 2个参数，参数ip 4. ping -c 3 8.8.8.8 貌似要根据服务器是windows还是linux而不同？5.忘了题目内容了 6.8.8.8.8&ls -la

其实就是DVWA里的Command Execution漏洞，学校里基本都会讲，学渗透的基本都熟悉这玩意吧

**试题三**

Wireshark抓包信息如下：



1.发起扫描源主机ip地址？

2.wireshark过滤上述ip的表达式？

3.判断扫描类型？

4.开放了哪些端口，判断过程？

5.有大量RST和ACK置位的网络分组，对于这种分组，其TCP标志字段的值为？

6.假设用iptables对上述扫描流量进行过滤，应该对filter表的哪条链上进行过滤，给出链的名字？

7.追加一条根据源IP地址丢弃上述网络流量的iptables的过滤规则？

【解说/吐槽】很常规的wireshark加iptables混合题，基本上大家应该都有复习到，算是送分题

**试题四**

[http://1.net](https://link.zhihu.com/?target=http%3A//1.net)系列命令中查看账户信息的完整命令？（2分）

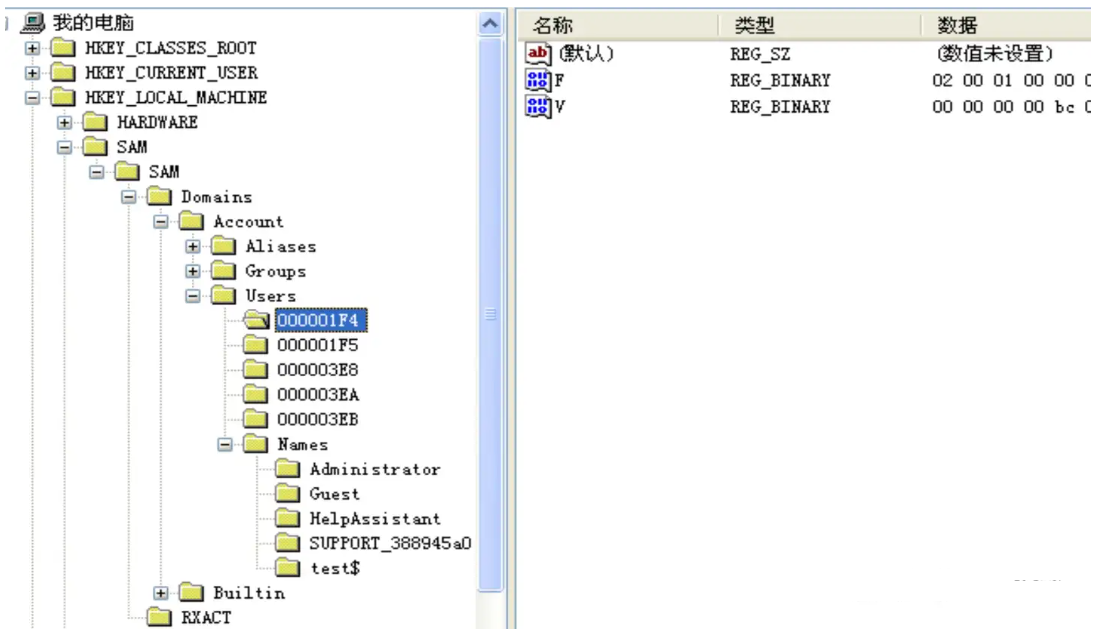
[http://2.net](https://link.zhihu.com/?target=http%3A//2.net)命令新建test$账户，口令为123456？（2分）

3.（1）使用net命令是否看到test$账户？

（2）发现隐藏账号的命令或方法？（3分）

4.（1）Windows中用户账户信息保存在注册表中的哪个键值？

（2）默认情况下，管理员有无权限查看SAM中的信息？（2分）



5.（1）管理员账户对应的“Users”键值下的哪一项？

（2）实现将用户“test$”克隆为管理员账户，应该赋值哪个键的值？

（3）使用克隆后的账户远程登录，登录后查询的是哪个账户？（6分）

whoami#

query user#

【解说/吐槽】1. net user 2. net user test$ 123456 /add 3.（1）不能，命令行看不到隐藏账户（2）注册表查看？4.（1）Users?（2）默认无权限，要设置才行 5.（1）000001F4？（2）F键的值（3）？

**试题五**

1.（1）APP打包后的格式？

（2）是否可以用zip扩展名进行替换并进行解压？

2.打包后的文件包括静态资源文件（assets）、库文件（lib）、签名文件（META-INF）、编译资源文件（res）、配置清单文件（AndroidManifest.xml）、核心代码文件（classes.dex）和资源映射文件（resources.arsc）等信息。（2分）

3.地图导航类软件最小必要权限？（2分）

4.保护APP安全性通常采用的安全保护措施中，包含以下哪几项？

A.防反编译 B.地址空间布局随机化 C.放调试 D.防篡改 E防窃取

5.APP组件有Activity，Service服务，Content Provider内容提供，BroadcastReceiver广播接收器四种（8分）

（1）<activity

android:[(1)]="true"

android:name=".other.ComponentActivity">

</activity>

（2）哪个组件导致敏感信息泄露，SQL注入？

（3）为了降低上述组件风险，安卓系统的permission检查机制可以控制一个应用APP拥有哪些执行权限？以常见的Activity为例。

<Permission

android:laber="允许打开webActivity页面权限"

android:name="com.littlejerk.sample.permission.WEB"

android:protectionLevel="signature"/>

其中protectionLevel="signature"表示受保护权限，除了上述signature以外还有哪两种保护等级？

（4）<(4)android:name="com.littlejerk.sample.permission.WEB"/>

完善上述权限申请