信息安全技能大赛

陕西工业职业技术学院选拔赛

赛竞试卷

**（满分100分，时间 120分钟）**

**竞赛注意事项：**

1. 禁止携带和使用移动存储设备、计算器、通信工具及参考资料。
2. 请按照以下比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。
3. 操作过程中，需要及时保存设备配置。比赛过程中，不要关闭任何设备，不要拆、动硬件连接。

一、**选择题：**本题共计25个，本题可能有一个或多个选项，每题1分 ，共计25分

1. 密码学的目的是（）。

A. 研究数据加密 B. 研究数据解密

C. 研究信息安全 D. 研究数据保密

2. “公开密钥密码体制”的含义是（）。

A. 将所有密钥公开 B. 将私有密钥公开，公开密钥保密

C. 将公开密钥公开，私有密钥保密 D. 两个密钥相同

3. 信息安全的基本属性是（）。

A. 机密性 B. 可用性

C. 完整性 D. 上面3项都是

4. Nmap进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是什么？ （ ）

A．文件服务器 B．邮件服务器

C．WEB服务器 D．DNS服务器

5. Telent服务默认运行在（ ）。

A．21 B．23 C．25 D．80

6. 不是计算机病毒所具有的特点()。

A 传染性 B 破坏性

C 潜伏性 D 可预见性

7. 防火墙最主要被部署在( )位置。

A桌面终端 B 骨干线路

C网络边界 D 重要服务器

8. 和进程完成自己的工作而又没有从事其他操作可能，这样能够使失误出错或蓄意袭击造成的危害降低，这通常被称为（）

A 适度安全原则 B 授权最小化原则

C 分权原则 D 木桶原则

9. 李欣打算从自己计算机保存的动画中挑选喜欢的发送给表姐欣赏，她应该从扩展名为()件中进行查找。

A、.mp3 B、.flv

C、.txt D、.xls

10. 2014年，互联网上爆出近几十万12306网站的用户信息，12306官方网站称是通过（）式泄露的。

A、拖库 B、撞库

C、木马 D、信息明文存储

11. 下列关于密码安全的描述，不正确的是（)

A、容易被记住的密码不一定不安全

B、超过12位的密码很安全

C、密码定期更换

D、密码中使用的字符种类越多越不易被猜中

12 软件供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个“后门”程序。以下哪一项是这种情况面临的最主要风险？（）

A、软件中止和远程监控

B、远程监控和远程维护

C、 软件中止和黑客入侵

D、远程维护和黑客入侵

13.经常通过计算机网络进行购物，从安全角度看，下面哪项是不好的操作习惯（）

A、在使用网络浏览器时，设置不在计算机中保留网络历史记录和表单数据

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

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、 用专用的计算机进行网上购物，安装好软件后不对该计算机上的系统软件、应用 件进行升级

14. 操作系统中\_\_\_\_文件系统支持加密功能（）

A、 NTFS B、 FAT32

C、 FAT D、EFS

15. 通过防火墙禁止QQ工具联网，应该修改Windows防火墙以下哪项设置()

A、 入站规则 B、 出站规则

C、 连接安全规则D、 监视

16. Windows server来宾用户登录主机时，默认用户名为：（）

A、 anonymous B、 admin

C、 root D、 guest

17. 访问以下哪个网址将可能遭受钓鱼攻击（）

A、 www.taobao.com

B、 www.qq.com

C、 www.1cbc.com.cn

D、 www.sina.com

18. 以下()带病毒或木马。

A．二维码 B．IP地址 C．微信用户名 D．微信群

19.交叉线的两端分别是（）

1. 标准558A、标准558B
2. 标准568A、标准568B
3. 标准578A、标准578B
4. 标准588A、标准588B

20.在命令与提示符下，如何查看本机网卡IP（）

1. Ifconfig
2. Systeminfo
3. Ipconfig
4. Ipaddress

**以下五道为多选题，多答或少答均得一半分，答错不得分**

21. 黑客攻击手段（ ）

A．暴力猜测 B．利用已知漏洞攻击

C．特洛伊木马 D．拒绝服务攻击

E．缓冲区溢出攻击 F．嗅探Sniffer

22. 户可以设置的文件属性有（）

A．只写

B. 隐藏

C. 存档

D. 只读

23. 黑客常用的获取关键账户口令的方法有：（）

A、通过网络监听非法得到用户口令

B、暴力破解

C、社工撞库

D、SSL协议数据包分析

24. 以下哪些行为可能导致操作系统产生安全漏洞()

A、使用破解版的编程工具

B、不安全的编程习惯

C、考虑不周的架构设计

D、编程计算机未安装杀毒软件

25. 以下哪些关于网络安全的认识是错误的？（）

A、电脑病毒的防治只能靠软件查杀；

B、文件删除后信息就不会恢复；

C、只要不连网就安全

D、防病毒软件要定期升级。

**二、填空题：**本题共计15个，每题1分，共计15分

* + - 1. Windows远程桌面默认运行在\_ \_\_端口
      2. SSH默认运行在\_\_ \_端口
      3. VPN全称叫\_\_ \_\_\_\_
      4. root用户的UID和GID都是\_\_\_\_
      5. Linux下移动文件位置的命令是\_\_ \_\_
      6. 直通线的线序是\_\_\_\_\_\_\_
      7. 在Windows命令与提示符中可以使用\_\_\_ \_\_命令查看全面查看系统信息
      8. \_ \_\_基于Debian的一个用于数字取证、渗透测试、黑客攻防Linux发行版
      9. FTP协议是一种用于\_\_\_的协议
      10. Ping长用来诊断\_\_\_\_\_\_
      11. 交换机上用于隔绝广播风暴的技术叫\_\_\_\_\_
      12. Linux中4,2,1是运行权限是\_\_\_\_\_\_
      13. 192.168.1.0/27 的子网掩码是\_\_\_\_
      14. 192.168.1.0/ 30 中有\_\_\_\_\_个子网
      15. 192.168.1.0/28 中有\_\_\_\_个主机

**三、判断题：**本题共计5个，每题1分, 填入（T）（F）

1. ls -a > > info命令能把ls -a执行后的回显示追加写入info文件中 ( )
2. Windows上的所有文件在Linux绝对不能运行 ( )
3. 登陆Linux系统只能使用密码 ( )
4. Linux每个文件和目录都有访问权限控制 ( )
5. 只靠技术就能够实现安全。 ()
6. /etc/shadow文件是用户访问控制配置文件 ()
7. 在Linux中可以用 init 0 关机 ( )
8. 用户可以用su命令切换用户身份 ( )
9. 用户可用grep命令查找特定字符串 ( )
10. 改变权限的命令为chown ( )

**四、操作题：**本题共计15小题，Linux部分15分（a,b,c 2分 d 4分e 5分）Windows部分30分(a,b,c,d,e.f 2分 g,h 4 分I,j 5分 )，请将需要截图操作步骤截图并贴进答题文档。

**Linux基础**

1. 请完成以下任务：
   1. 新建一个用户，为其设置密码
   2. 查看其UID、GID、默认用户组、禁止其登录shell。
   3. 新建一个目录dir 修改其所有者和所属组划分给你所新建的用户和默认组
   4. 调整权限为所有者：读、写、执行权限，组读、写、执行权限，其他人可读、不可写、不可执行权限。
   5. 配置你新建的用户密码有效期为30天

答案:

**Windows基础**

1. 请完成以下任务：
   1. 禁用Guest账号，并改名
   2. 把系统Administrator账号改名
   3. 创建一个陷阱用户,
   4. 配置账户锁定策略，3次密码错误，锁定1小时。重置设为10080分钟。配置不显示最后的用户名。配置密码复杂性要求（设置密码长度最小值为10位 ，设置强制密码历史为5次，时间为30天），并使用简单口令进行测试。
   5. 安装IIS，并在浏览器中访问
   6. 将IIS目录与系统磁盘分开，保存在专用磁盘空间内。删除多余映射(asp, aspx , html, htm) 并配置Web站点权限设定，主目录：读取 允许，写入 不允许：脚本源访问 不允许：目录浏览 关闭：日志访问 关闭：索引资源 关闭：执行 纯脚本
   7. 查看Window默认共享并添加本地策略组中开机时删除此共享(net share 盘符$ /del)
   8. 更改Windows防火墙的日志(firewall.txt)默认储存改到位置为C:\Windows\_sec\_log 目录，勾选所有记录选项
   9. 把以下代码保存为server\_info.bat 放C:\Windows\_sec\_log下，新建任务计划定时运行此批处理，并定时把生成的info.txt 作为邮件附件将这些每隔24小时发往test@test.com

@tasklist > info.txt

@netstat -ano >> info.txt

@type firewall.txt >> info.txt

* 1. 配置只允许你所在的主机的IP地址连接远程桌面，并连接

**五、简答题：**

1. 假如你是某单位的渗透工程师实习生，接到的渗透的目标网站中你发现存在MySQL 注入漏洞，你如何进一步的发现更多的信息。并向你的主管报告此漏洞的修复方法（无需提供任何代码，提供你的渗透思路即可）

答：