# 2022 年大学生网络安全知识竞赛题库及答案（共 70 题）

1. WINDOWS 系统，下列哪个命令可以列举本地所有用户列表

A.netuser

B.netview

C.netname

D.netaccounts

A

2. WINDOWS 系统，下列哪个命令可以列举出本地所有运行中的服务

A.netview

B.netuse

C.netstart

D.netstatistics

C

3. ORACLE 的默认通讯端口有哪些？

A、TCP1521

B、TCP1025

C、TCP1251

D、TCP1433

A

4. 一般网络设备上的 SNMP 默认可读团体字符串是：

A.PUBLIC

B.CISCO

C.DEFAULT

D.PRIVATE

A

5. 一般来说，路由器工作在 OSI 七层模式的哪层？

A、三层，网络层

B、二层，数据链路层

C、四层，传输层

D、七层，应用层

答：

A

6. 黑客通常实施攻击的步骤是怎样的？

A、远程攻击、本地攻击、物理攻击

B、扫描、拒绝服务攻击、获取控制权、安装后门、嗅探

C、踩点（包括查点）、扫描、获取访问权、提升权限、安装后门、清除痕迹

C

7. solaris 的用户密码文件存在在哪个文件中？

A、/etc/passwd

B、/etc/shadow

C、/etc/security/passwd

D、/etc/password

答：

B

8. 某文件的权限为“-rwxrw-r—”，代表什么意思？

A、管理员可读写及可执行，管理员组用户可读写，其他用户可读

B、管理员可读，管理员组用户可读写，其他用户可读写及可执行

C、管理员可读写及可执行，其他用户可读写，管理员组用户可读

D、管理员可读写，管理员组用户可读，其他用户可读写及可执行

A

9. SSH 使用的端口号是多少？

A、21

B、22

C、23

D、4899

答：

B

10. 在信息系统安全中，风险由以下哪两种因素共同构成的？

A. 攻击和脆弱性

B. 威胁和攻击

C. 威胁和脆弱性

D. 威胁和破坏

C

11. 关闭 cisco 网络设备的 echo 服务，应该使用哪个命令：

A. noservicetcp -small-servers

B. noiptcp -small-servers

C. noservicetcp -small-services

D. notcp-small-servers

A

12. 在 cisco 网络设备中，以下对于访问控制列表应用的顺序，说法错误的是：

A. 从控制列表的第一条顺序查找，直到遇到匹配的规则

B. 默认有 deny 的规则

C. 细致的规则匹配优先于概括的规则匹配，比如 192.168.10.0/24 的匹配优先于 192.168.0.0/16 的匹配

C

13. 在 Solaris 操作系统中，不必要的服务应该关闭。Solaris 需要关闭的服务，一般配置在，以下最准确的答案是：

A. /etc/inetd.conf 文件和/etc/rc*.d/ 中

B. /etc/resolv.conf 中

C. /etc/services

A

14. 根据以下/etc/passwd 文件，具有超级用户权限的用户是：

```
bash-2.03# cat passwd
root:x:0:1:Super-User:/:/bin/bash
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:0:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
```

A、 只有 root

B、 只有 bin

C、 只有 adm

D、 以上都不对

D

15. 某系统的/.rhosts 文件中，存在一行的内容为“++”，并且开放了 rlogin 服务，则有可能意味着：

A. 任意主机上，只有 root 用户可以不提供口令就能登录该系统

B. 任意主机上，任意用户都可以不提供口令就能登录该系统

C. 只有本网段的任意用户可以不提供口令就能登录该系统

D. 任意主机上，任意用户，都可以登录，但是需要提供用户名和口令

B

16. 如果 /etc/syslog.conf 中，包含以下设置：“auth.warning /var/adm/auth.log”，则以下说法可能正确的是：

A. /var/adm/auth.log 将仅仅记录 auth 的 warning 级别的日志

B. /var/adm/auth.log 将记录 auth 的 emerg、alert、crit、err、warning

级别的日志

C. /var/adm/auth.log 将记录 auth 的 warning、notice、info、debug 级别的日志

B

17. 一台 Windows2000 操作系统服务器，安装了 IIS 服务、MSSQLServer 和 Serv-UFTPServer，管理员通过 MicrosoftWindowsUpdate 在线安装了 Windows2000 的所有安全补丁，那么，管理员还需要安装的补丁是：

A. IIS 和 Serv-UFTPServer

B. MSSQLServer 和 Serv-UFTPServer

C. IIS、MSSQLServer 和 Serv-UFTPServer

D. 都不需要安装了

B

18. 以下 Windows2000 注册表中，常常包含病毒或者后门启动项的是：

A.

B.

C.

D.

B

19. 做系统快照，查看端口信息的方式有：

A、 netstat–an

B、 netshare

C、 netuse

D、 用 taskinfo 来查看连接情况

A

20. 地址解析协议 ARP 的作用是（）。

A、IP 地址转换为设备的物理地址

B、将设备的物理地址转换为 IP 地址

C、将域名转换为 IP 地址

D、将 IP 地址转换为域名

A

21. 下面哪一种不是防火墙的接口安全选项

A．防代理服务 B．防 IP 碎片 C．防 IP 源路由 D．防地址欺骗

A

22. 下列说法错误的是：

A. 防火墙不能防范不经过防火墙的攻击

B. 防火墙不能防范基于特殊端口的蠕虫

C. 防火墙不能防止数据驱动式的攻击

B

23. 下列哪个是能执行系统命令的存储过程

A.Xp_subdirsB.Xp_makecabC.Xp_cmdshellD.Xp_regread

C

24. “Select*fromadminwhereusername= ‘admin’andpassword= ‘”

&request( “pass”)& “’ ”如何通过验证

A.‘1’or‘1’=‘1’B.1or1=1C.1’or‘1’=‘1D.‘1’=‘1’

C

25. “Select*fromNewswherenew_id= ”

&replace(request( “newid”,”’”,”” )”是否存在注入？

A.是 B.否

A

26. 从数据来源看，入侵检测系统主要分为哪两类

B、主机型、混合型

C、网络型、主机型

D、主机型、诱捕型

C

协议的 4 层概念模型是(单选)

A、应用层、传输层、网络层和网络接口层

B、应用层、传输层、网络层和物理层

C、应用层、数据链路层、网络层和网络接口层

D、会话层、数据链路层、网络层和网络接口层

(A)

28. 在 UNIX 系统中，当用 ls 命令列出文件属性时，如果显示 -rwxrwxrwx，意思是（）

A、前三位 rwx 表示文件属主的访问权限；中间三位 rwx 表示文件同组用户的访问权限；后三位 rwx 表示其他用户的访问权限

B、前三位 rwx 表示文件同组用户的访问权限；中间三位 rwx 表示文件属主的访问权限；后三位 rwx 表示其他用户的访问权限

C、前三位 rwx:表示文件同域用户的访问权限；中间三位 rwx 表示文件属主的访问权限；后三位 rwx:表示其他用户的访问权限

rwx 表示文件属主的访问权限；第二个 rwx 表示文件同组用户的访问权限；后三位 rwx 表示同域用户的访问权限

(A)

中，默认的共享文件系统在哪个位置（）

A、/sbin/

B、/use/local/

C、/export/

D、/usr/

(C)

30. 通过以下哪个命令可以查看本机端口和外部连接状况()

A、netstat－an

B、netconn-an

C、netport-a

D、netstat-all

A

31. LINUX 中，什么命令可以控制口令的存活时间？（）

chage

B、passwd

C、chmod

D、umask

(A)

系统中存放每个用户的信息的文件是（）

A、/sys/passwd

B、/sys/password

C、/etc/password

D、/etc/passwd

（D）

33. linux 系统中如何禁止按 Control-Alt-Delete 关闭计算机(单选)

A、把系统中“/sys/inittab”文件中的对应一行注释掉

B、把系统中“/sysconf/inittab”文件中的对应一行注释掉

C、把系统中“/sysnet/inittab”文件中的对应一行注释掉

D、把系统中“/sysconf/init”文件中的对应一行注释掉

(B)

34. 由于 ICMP 消息没有目的端口和源端口，而只有消息类型代码。

通常过滤系统基于（）来过滤 ICMP 数据包（单选）

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/878014020013006101