1. 如果不使用地址空间随机化，代码段和数据段是彼此相连的，使用地址空间随机化的一个目的是降低栈溢出攻击的风险。
2. GOT和PLT是数据段的一部分，可以用来实现位置无关代码的重定位
3. Linux系统调用返回-1代表出现错误
4. 内核会安排init进程作为所有孤儿进程的养父，init的进程的pid为1，是在系统启动时由内核创建的
5. SIGKILL和SIGSTOP既不能被捕获也不能被忽略
6. 在使用kill(pid,signal)发送信号时，若pid>0表示向进程号为pid的进程发送信号，而若pid<0表示向进程号为|pid|的进程所在的进程组发送信号
7. 在信号处理程序中只在处理程序会返回时有必要保存和恢复errno
8. 我们使用Signal包装函数来保证信号处理语义的一致性，这个包装函数约定会尽可能重启被中断的系统调用
9. 由于setjmp的返回值不能赋值给变量，因此也无法用在switch等条件分支语句的测试中
10. 如同fork一样，setjmp也会调用一次但可能返回多次，此时可以根据其返回值判断其是第一次返回还是从longjmp返回
11. 一个目录至少包含一个链接：..表示到目录层次结构中父目录的链接。/表示根目录
12. 调用open时如果使用O\_CREAT会自动创建一个不存在的文件，但若文件已经存在则会将文件截断
13. 有缓冲区的rio函数可以交替调用用来读文本和二进制混合的文件，但不应和无缓冲区的rio函数混合调用，每次打开一个文件描述符都要用rio\_readinitb函数初始化一个缓冲区
14. 可以用stat和fstat读取文件元数据，stat以文件描述符为输入，fstat以文件名为输入
15. 在使用dup2(oldfd,newfd)的过程中会先将打开的newfd关闭，再将oldfd的信息复制给newfd，因此要求原先的newfd必须是已经打开的文件描述符
16. 每个以太网适配器有全球唯一的32位地址，存储在易失性存储器上
17. 每个以太网适配器有全球唯一的48位地址，存储在易失性存储器上
18. 集线器和网桥会不加甄别的将收到的所有位发送给连接的每一个端口
19. 在使用路由器进行不兼容的局域网络间的数据传送时，一个互联网络包的有效载荷应当是一个帧，而一个帧的有效载荷是真正要传送的数据
20. IPV4使用32位地址，而IPV6使用64位地址
21. 一个套接字是连接的一个端点，每个套接字有相应的套接字地址，由一个因特网地址和一个16位整数端口（与适配器端口相对应）组成。
22. 域名层次形成了一个树形结构，从根节点到某一叶节点的路径构成了一个域名，有且仅有根节点在树的第一层。
23. 套接字接口与套接字端口是不同的，在Linux中套接字接口是一组函数
24. 试默写客户端与服务器通信的模型流程图
25. 在getaddrinfo和getnameinfo函数中都有两个参数host与service，二者都可以设置成NULL，但不能同时设置成NULL
26. 如果我们希望getaddrinfo对每个地址只返回一个addrinfo结构，那么我们应当将ai\_socktype参数设置成SOCK\_STREAM
27. 在open\_listenfd函数中，我们调用getaddrinfo时需要使用AI\_PASSIVE标志并将host设为NULL，这样得到的套接字地址结构中的地址字段是通配符地址，可以接受发送到该主机所有IP地址的请求。
28. 一个可执行文件的URL可以用&来分隔文件名和参数，用?来分隔各个参数，用%20来表示空格，URL中不能出现空格
29. URL后缀中的/不表示根目录，最小的URL后缀就是/，服务器会默认将其扩展为空页面
30. GET指导服务器生成和返回URI标识的内容，对于使用代理的请求，URI是对应URL表示文件名和参数的后缀
31. 在请求动态内容时，服务器fork一个子进程，并在execve之前按传递的参数设置环境变量，然后运行CGI程序，CGI程序会将其标准输出重定向到客户端相关联的已连接描述符，这样CGI写到标准输出的内容会直接发送到客户端。
32. 出于安全的考虑，在CGI程序中不应当使用标准I/O函数，而应当使用健壮的读写函数