00:32:45　　共50题　　合计100分

1、 50.SQLSERVER数据库身份验证支持的模式是

（单选题，2分）

- A. SQL身份验证模式
- B. windows和SQL混合验证模式
- C. windows身份验证模式
- D. radius身份验证模式

2、 49.Mysql数据库若使用load_file()函数读取操作系统文件时需要的权限是

（单选题，2分）

- A. Write
- B. LoadFile
- C. File
- D. Read

3、 48.在测试sql注入时，以下哪种方式不可取

（单选题，2分）

A. ?id=1 or 1=1

B. ?id=2-1

C. ?id=1+1

D. ?id=1 and 1=1?id=1 and 1=1

4、 47.默认情况下，windows的哪个版本可以抓取到LM hash

（单选题，2分）

A. windows XP

B. windows server 2008

C. windows Vista

D. windows 7

5、 46.一个网站存在命令执行漏洞，由于服务器不能连外网，这时我们可以利用什么样的方式将文件上传到服务器

（单选题，2分）

A. Vbs

B. powershell

C. Echo

D. ftp

6、 45.如果一个网站存在CSRF漏洞，可以通过CSRF漏洞做什么？

（单选题，2分）

A. 获取网站用户注册的个人资料信息

B. 修改网站用户注册的个人资料信息

C. 冒用网站用户的身份发布信息

D. 以上都可以

7、 44.当访问web网站的某个页面资源不存在时，将会出现的HTTP状态码是？

（单选题，2分）

A. 200

B. 404

C. 201

D. 302

8、 43.在以下认证方式中，最常用的认证方式是：

（单选题，2分）

A. 基于帐户名/口令认证

B. 基于PKI认证

C. 基于摘要算法认证

D. 基于数据库认证

9、 42.数据保密性安全服务的基础是

（单选题，2分）

A. 数字签名机制

B. 加密机制

C. 访问控制机制

D. 数据完整性机制

10、 41.信息安全“老三样” 是？

（单选题，2分）

A. 防火墙、入侵检测、扫描

B. 防火墙、扫描、杀毒

C. 入侵检测、扫描、杀毒

D. 防火墙、入侵检测、杀毒

11、 10.linux 环境下，查询日志文件最后100行数据，正确的方式是

（单选题，2分）

A. grep -100 log

B. mv -100 log

C. tail -100 log

D. cat -100 log

12、 9.以下命令可以用来获取DNS记录的是

（单选题，2分）

A. dig

B. ping

C. who

D. traceroute

13、 8.以下哪个数据库不是关系型数据库

（单选题，2分）

A. mysql

B. mssql

C. redis

D. oracle

14、 7.以下数据库只能通过字典枚举数据表的是

（单选题，2分）

A. mysql < 5.0

B. mysql > 5.0

C. oracle

D. mssql

15、 6.以下哪个工具不可以抓取HTTP数据包

（单选题，2分）

A. Nmap

B. Fiddle

C. Burpsuite

D. Wireshark

16、 5.向有限的空间输入超长的字符串是哪一种攻击手段

（单选题，2分）

A. 缓冲区溢出

B. IP欺骗

C. 拒绝服务

D. 网络监听

17、 4.主要用于加密机制的协议是

（单选题，2分）

A. SSL

B. TELNET

C. HTTP

D. FTP

18、 3. 下列哪类工具是日常用来扫描web漏洞的工具

（单选题，2分）

A. NMAP

B. IBM APPSCAN

C. X-SCAN

D. Nessus

19、 2.常规端口扫描和半开放式扫描的区别是

（单选题，2分）

A

A. 半开式采用UDP方式扫描

B. 没区别

C. 扫描准确性不一样

D. 没有完成三次握手，缺少ACK过程

20、 1. 张三将微信个人头像换成微信群中某好友头像，并将昵称改为该好友的昵称，然后向该好友的其他好友发送一些欺骗消息。该攻击行为属于以下哪类攻击

（单选题，2分）

A. 口令攻击

B. 拒绝服务攻

C. 社会工程学攻击

D. 暴力破解

21、 20. ARP欺骗的实质是

（单选题，2分）

A. 让其他计算机知道自己的存在

B. 窃取用户在网络中传输的数据

C. 扰乱网络的正常运行

D. 提供虚拟的MAC与IP地址的组合

22、 19.TCP SYN 泛洪攻击的原理是利用了

（单选题，2分）

A. TCP三次握手过程

B. TCP连接终止时的FIN报文

C. TCP数据传输中的窗口技术

D. TCP面向流的工作机制

23、 18.在以下的认证方式中，最不安全的是

（单选题，2分）

A. SPAP

B. MS-CHAP

C. CHAP

D. PAP

24、 17.SQL杀手蠕虫病毒发作的特征是什么

（单选题，2分）

A. 攻击手机网络

B. 攻击个人PC终端

C. 大量消耗网络带宽

D. 破坏PC游戏程序

25、 16.网络攻击的发展趋势是

（单选题，2分）

A. 黑客攻击

B. 黑客技术与网络病毒日益融合

C. 病毒攻击

D. 攻击工具日益先进

26、 15.Windows操作系统中可显示或修改任意访问控制列表的命令是

（单选题，2分）

A. systeminfo

B. ipconfig

C. cacls

D. tasklist

27、 14.反向连接后门和普通后门的区别是

（单选题，2分）

A. 根本没有区别

B. 主动连接控制端、防火墙配置不严格时可以穿透防火墙

C. 只能由控制端主动连接，所以防止外部连入即可

D. 这种后门无法清除

28、 13.TCP会话劫持出了SYN Flood攻击，还需要

（单选题，2分）

A. SYN扫描

B. 序列号预测

C. 扫描TCP

D. 扫描SYN/ACK

29、 12.攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息，重放发往B称为

（单选题，2分）

A. 口令猜测器和字典攻击

A. 命令清洗器和字典攻击

B. 回放攻击

C. 强力攻击

D. 中间人攻击

30、 11.下面哪个是administrator用户的SID

（单选题，2分）

A. S-1-5-21-3698344474-843673033-3679835876-100

B. S-1-5-21-3698344474-843673033-3679835876-1001

C. S-1-5-21-3698344474-843673033-3679835876-500

D. S-1-5-21-3698344474-843673033-3679835876-1000

31、 30.在编写目录扫描工具时哪种请求方式可以增加扫描速度

（单选题，2分）

A. GET

B. PUT

C. HEAD

D. POST

32、 29.下面的哪个命令可以打印linux下的所有进程信息

（单选题，2分）

A. Su

B. ls -l

C. ps -ef

D. ls -d

33、 28.数据完整性指的是

（单选题，2分）

A. 防止非法实体对用户的主动攻击，保证数据接收方收到的信息与发送方发送的信息完全一致

B. 保护网络中个系统之间交换的数据，防止因数据被截获而造成泄密

C. 确保数据是由合法实体发出的

D. 提供连接实体身份的鉴别

34、 27.Oracle默认情况下，口令的传输方式是

（单选题，2分）

A. DES加密传输

B. 明文传输

C. 3DES加密传输

D. MD5加密传输

35、 26.依据OSI安全体系结构，数据链路层能提供？

（单选题，2分）

A. 数据完整性服务

B. 抗抵赖性服务

C. 鉴别服务

D. 连接机密性服务

36、 25.之前版本的中间件未出现过解析漏洞的是

（单选题，2分）

A. Tomcat

B. apache

C. Iis

D. ngnix

37、 24.攻击者通过XSS漏洞获取到QQ用户的cookie后，可以进行一下操作？

（单选题，2分）

A. 劫持微信用户

B. 偷取Q币

C. 控制用户摄像头

D. 进入QQ空间

38、 23.Firefox浏览器插件Hacbar提供的功能没有什么？

（单选题，2分）

A. 修改浏览器访问referer

B. BASE64编码和解码

C. 代理修改WEB页面的内容

D. POST方式提交数据

39、 22.许多黑客攻击都是利用软件实现中的缓冲区溢出的漏洞，对此最可靠的解决方案是什么？

（单选题，2分）

A. 安装防病毒软件

B. 安装防火墙

C. 给系统安装最新的补丁

D. 安装入侵检测系统

40、 21.以下算法中属于非对称算法的是

（单选题，2分）

A. DES

B. RSA算法

C. IDEA

D. 三重DES

41、 40.下列那个选项不是上传功能常用安全监测机制？

（单选题，2分）

A. URL中是否包含一些特殊标签<、>、script、alert

B. 服务的MIME检查验证

B. 服务器端检查验证

C. 服务端文件扩展名检查验证机制

D. 客户端检查机制JavaScript验证

42、 39.黑客通常实施攻击的步骤是什么？

（单选题，2分）

A. 扫描、拒绝服务攻击、获取控制权、安装后门、嗅探

B. 拒绝服务攻击、扫描、获取控制器、清除痕迹

C. 远程攻击、本地攻击、物理攻击

D. 踩点、扫描、获取访问权、提升权限、安装后门、清除痕迹

43、 38.XXE漏洞可以做什么

（单选题，2分）

A. 获取用户浏览器信息

B. 网络钓鱼

C. 盗取用户cookie

D. 读取服务器文件

44、 37.如何防护存储型XSS漏洞？

（单选题，2分）

A. 使用Cookie存储身份信息

B. 对html标签进行转义处理

C. 使用Ajax技术

D. 使用安全的浏览器

45、 36.以下关于VPN说法正确的是

（单选题，2分）

A. 进入QQ空间VPN只能提供身份认证、不能提供加密数据的功能

B. VPN指的是用户通过公用网络建立的临时的、安全的连接

C. VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

D. VPN不能做到信息认证和身份认证

46、 35.以下哪个服务器未曾被发现文件解析漏洞？

（单选题，2分）

A. Nginx

B. squid

C. Apache

D. IIS

47、 34.以下关于cc攻击说法的

（单选题，2分）

A. cc攻击利用的时tcp协议的缺陷

B. cc攻击需要借助代理进行

C. cc攻击难以获取目标机器的控制权

D. cc攻击最早在国外大面积流行

48、 33.黑客通过以下哪种攻击方式，可能大批量获取网站注册用户的身份信息

（单选题，2分）

A. 越权

B. XSS

C. CSRF

D. 以上都可以

49、 32.SQL Sever中可以使用哪个存储过程调用操作系统命令，添加系统账号？

（单选题，2分）

A. xp_dirtree

B. xp_xshell

C. xp_cmdshell

D. xpdeletekey

50、 31.防止重发攻击最有效的方法是？

（单选题，2分）

A. 使用"一次一密"加密方式

B. 对用户账号和密码进行加密

C. 使用复杂的账号名称和密码

D. 经常修改用户账号名称和密码

提交试卷