考试: 正式比赛

团队: 北京邮电大学 名字: 孙艺祺 用户: 393214201@qq.com 开放时间: 2018-11-15 14:03:22 关闭时间: 2018-11-15 16:21:44 时间: 02:18:22 基本分值: 0.400 分数: 80.000 / 100.000 (80%)	正式比赛

#	分数	开始 [时:分:秒]	结束 [时:分:秒]	时间 [分:秒]
1 S	0.400	14:03:22	14:03:45	00:23

下列哪些不属于黑客地下产业链类型

+	1	移动互联网金融产业链
	2	网络虚拟资产盗窃地下产业链
	3	互联网资源与服务滥用地下产业链
	4	真实资产盗窃地下产业链

2 S	0.400	14:03:45	14:04:02	00:17

网站域名发生劫持，下列哪一项处理措施是错误的？

+	1	紧急关停网站
	2	联系域名注册商处理，或取回控制权自己修改为正确的IP
	3	更改与域名相关的所有帐户的密码
	4	针对搜索引擎中检索网站结果中的非法信息链接，进行快照投诉

3 S	0.400	14:04:02	16:15:20	11:18

下列关于回声隐藏算法描述不正确的是

	1	可以使用自相关检测回声提取0、1比特，但由于信号自身的相关性，回声延迟过小时，其相关度的峰值容易被淹没。
	2	回声隐藏算法的特点是听觉效果好，抗滤波重采样等攻击能力强，但嵌入容量不大。
+	3	一般使用倒谱自相关检测回声延迟，因为其准确度高，且算法复杂度低。
	4	回声隐藏算法利用时域掩蔽效应，在原声中叠加延迟不同的回声代表0、1比特。

4 S	0.400	16:15:20	16:15:22	00:02

WAF的全称是Web Application Firewall，关于常见的waf，以下说法错误的是？

+	1	对于任意长度的数据请求，waf都会进行检测
	2	可以使用数据库的空白字符如%09,%0a,%0b,%0c,%0d,%a0来绕过waf
	3	WAF可以以硬件、软件、或者云的形式存在
	4	WAF运行在TCP/IP的应用层

5 S	0.400	16:15:23	16:15:27	00:04

以下哪项工作最能确保风险评估后的纠正措施得到了有效落实？

+	1	进行跟进检查工作
	2	开展月度报告工作来验证纠正措施是否实施
	3	检查纠正措施是否得到了书面记录
	4	对负责纠正措施的员工进行访谈

6 S	0.400	16:15:27	16:15:32	00:05

以下对APT(AdvancedPersistentThreat)特征描述不准确的是。

	1	工具箱式的攻击工具集合
	2	隐蔽性高，不急于求成
	3	通常会利用0day漏洞
+	4	以感染尽可能多的终端为目的

7 S	0.400	16:15:32	16:15:35	00:03

在linux系统下，下列哪个日志文件最可能包含了入侵者的shell命令操作？

解释

解析：1 对日志系统的了解

+	1	history日志
	2	lastlog日志
	3	wtmp日志
	4	utmp日志

8 S	0.400		16:15:35	16:15:37	00:02
下列哪类工具是日常用来扫描web漏洞的工具					
	1	X-SCAN			
		解释 多线程方式对指定IP地址段(或单机)进行安全漏洞检测"			
+	2	AWVS			
	3	Nessus			
	4	NMAP			

9 S	0.400		16:15:37	16:15:48	00:11
拒绝服务攻击导致的危害中，以下哪个说法是不正确的					
+	1	应用系统被破坏，应用无法响应请求			
	2	应用资源被耗尽，应用无法响应请求			
	3	主机资源被耗尽，主机无法响应请求			
	4	网络带宽被耗尽，网络被堵塞，无法访问网络			

10 S	0.400		16:15:48	16:15:53	00:05
为了使得系统部署升级和配置更为方便以应对安全更新和安全加固配置，我们通常会使用自动化部署工具来节省部署时间，以下哪个不是自动化部署工具					
+	1	CookMaster			
	2	Puppet			
	3	SaltStack			
	4	Ansible			

11 S	0.000		16:15:53	16:15:56	00:03
以下哪个问题不是导致 DNS 欺骗的原因之一					
	1	DNS 协议是缺乏严格的认证			
	2	为提高效率，DNS 查询信息在系统中会缓存			
	3	DNS 协议传输没有经过加密的数据			
-	4	DNS 是一个分布式的系统			

12 S	0.400		16:15:56	16:15:59	00:03
为了有效的对企业网络进行安全防护，在企业网络的最外围部署防火墙是为了。					
	1	主动追踪攻击者来源			
+	2	隐藏网络内部细节			
	3	发现黑客攻击行为			
	4	记录用户的上网行为			

13 S	0.400		16:15:59	16:16:05	00:06
从kill chain来看，哪个阶段最难得到攻击者画像？					
		解释 解析：1 考察国际上网络攻防的基本概念			
	1	Delivery			
	2	Command &Control			
+	3	Reconnaissance			
	4	Exploit			

14 S	0.400		16:16:05	16:16:07	00:02
业务影响分析的关键指标为。					
	1	系统恢复优先级			
	2	数据重要程度			
+	3	RTO/RPO			
	4	业务中断造成的损失			

15 S	0.400		16:16:07	16:16:10	00:03
( )是一个对称DES加密系统，它使用一个集中式的专钥密码功能，系统的核心是KDC					
	1	TACACS			
+	2	Kerberos			
	3	PKI			
	4	RADIUS			

16 S	0.400		16:16:10	16:16:13	00:03
下列哪种措施是磁介质上信息擦除的最彻底形式					

解释 解析：磁介质需要消磁		
+	1	消磁
	2	文件粉碎
	3	删除
	4	格式化

17 S	0.400	16:16:13	16:16:16	00:03
SQL Server默认的通讯端口为以下哪个端口，为提高安全性建议将其修改为其他端口				
解释 解析：基本概念				
+	1	TCP 1433		
	2	TCP 1522		
	3	TCP 1521		
	4	TCP 1434		

18 S	0.400	16:16:16	16:16:19	00:03
不属于黑客被动攻击的是				
+	1	缓冲区溢出		
	2	打开病毒附件		
	3	浏览内嵌恶意代码网页		
	4	运行恶意软件		

19 S	0.400	16:16:19	16:16:23	00:04
《中华人民共和国保守国家秘密法》第二章规定了国家秘密的范围和密级，国家秘密的密级分为				
	1	“低级”、“中级”、“高级”三个级别。		
	2	“绝密”、“机密”、“秘密”、“公开”四个级别。		
+	3	“绝密”、“机密”、“秘密”三个级别。		
	4	“普通”、“商业”、“军事”三个级别。		

20 S	0.400	16:16:23	16:16:25	00:02
本地电脑使用下列哪个命令不能获取网站域名解析的IP地址？				
	1	Tracert		
+	2	Netstat		
	3	Nslookup		
	4	Ping		

21 S	0.400	16:16:25	16:16:28	00:03
以下哪个不是应用层防火墙的特点				
解释 解析：应用层防火墙速度并不快。				
	1	更有效的防止应用层的攻击		
	2	比较容易进行审计		
+	3	线速处理且对用户透明		
	4	工作在OSI模型的第七层		

22 S	0.400	16:16:28	16:16:39	00:11
向一个二进制文件中写入信息的函数为				
	1	fread()		
	2	fgets()		
	3	fputs()		
+	4	fwrite()		

23 S	0.000	16:16:33	16:16:47	00:14
在信息安全工作中，安全与发展的关系是。				
	1	安全优先，发展中求安全		
-	2	安全与发展并重，确保安全		
	3	以安全保发展，在发展中求安全		
	4	发展优先，以发展带动安全		

24 S	0.400	16:16:47	16:16:52	00:05
以下属于不属于对称加密算法的是				

	1	DES
	2	RC4
+	3	SHA-1
	4	3DES

25 S	0.400	16:16:52	16:16:57	00:05

下列哪个工具可以在最短的时间内对全球所有已分配的IPv4地址进行指定端口扫描

解释

解析：ZMAP是一款新型的扫描工具，通过绕过系统协议栈和并发可以实现超高速的地址和端口扫描功能，据说可以44分钟内扫描完全球的IPv4地址。

	1	NMAP
	2	HPING3
	3	HMAP
+	4	ZMAP

26 S	0.400	16:16:57	16:17:01	00:04

下面哪种不属于防火墙部属方式:

+	1	网络模式
	2	透明模式
	3	混合模式
	4	路由模式

27 S	0.400	16:17:01	16:17:14	00:13

以下哪种手段可以更有效应对较大范围的安全事件的不良影啊，保证关键服务和数据的可用性？

	1	定期备份
+	2	异地备份
	3	本地备份
	4	人工备份

28 S	0.400	16:17:14	16:17:17	00:03

linux特殊权限不包含下列哪个？

解释

解析：3 对linux特殊权限的了解

	1	SGID
+	2	SOID
	3	SBIT
	4	SUID

29 S	0.400	16:17:17	16:17:20	00:03

Linux防火墙有丰富的判定选项，下列哪个不属于Linux防火墙的判定选项：

	1	接口名
	2	TCP标志位
+	3	进程ID
	4	源IP地址

30 S	0.400	16:17:20	16:17:24	00:04

入侵检测技术可以分为误用检测和两大类。

	1	病毒检测
	2	漏洞检测
+	3	异常检测
	4	详细检测

31 S	0.400	16:17:24	16:18:10	00:46

上载文件的保护以下哪个是最为安全的

	1	上载文件放到Web的uploads目录内，使用较长的GUID重命名文件，以避免被黑客枚举
+	2	上载文件放在Web的目录外，对文件进行保护，在下载文件时只写x_sendfile字段，由Apache2、Nginx返回
	3	上载文件放到Web的uploads目录内，使用Url重写机制，对文件进行保护，在下载文件之前判断用户的Session权限
	4	上载文件放在Web的目录外，对文件进行保护，在下载文件之前通过读入文件数据并直接返回给浏览器

32 S	0.400	16:18:10	16:18:14	00:04

下面哪个X86指令用于产生中断？

解释

解析：2 对X86指令的了解		
+	1	int 3
	2	push ebp
	3	ret 4
	4	nop

33 S	0.400	16:18:14	16:18:17	00:03
木马程序为了实现其特殊功能，一般不应具有哪种性质				
解释 解析：木马通常以各种伪装技术隐藏自身进行窃取用户信息等非法活动，为了防止用户察觉通常不破坏宿主计算机系统。				
	1	隐藏性		
	2	窃密性		
+	3	破坏性		
	4	伪装性		

34 S	0.400	16:18:17	16:18:20	00:03
下面哪一项最好地描述了组织机构的安全策略？				
	1	表明所使用的技术控制措施的高层陈述		
	2	表明管理意图的高层陈述		
	3	建议了如何符合标准		
+	4	定义了访问控制需求的总体指导方针		

35 S	0.400	16:18:20	16:18:23	00:03
在信息安全保障体系中，最重要的核心组成部分为。				
	1	应急与保障体系		
	2	技术体系		
+	3	管理体系与安全策略		
	4	教育与培训		

36 S	0.400	16:18:23	16:18:25	00:02
通过在HTTP Header里面设置X-Frame-Options可以预防下面哪个问题				
	1	XSS		
	2	XXE		
	3	CSRF		
+	4	Clickjacking		

37 S	0.400	16:18:25	16:18:33	00:08
以下不属于防火墙的组成要素的是				
+	1	加密措施		
	2	内部网		
	3	安全策略技术手段		
	4	外部网		

38 S	0.400	16:18:33	16:18:34	00:01
下面哪个伪协议能用于读取php文件				
	1	phar://		
	2	php://input		
+	3	php://filter		
	4	zip://		

39 S	0.000	16:18:34	16:18:52	00:18
为应用设计访问控制机制时一般不包括。				
	1	会话管理机制		
	2	认证机制		
-	3	隐私保护机制		
	4	授权机制		

40 S	0.400	16:18:52	16:18:53	00:01
下列RAID磁盘阵列部署过程中，哪一项至少需要的硬盘数为4个？				
	1	RAID5		
+	2	RAID0+1		
	3	RAID0		

	4	RAID3	

41 S	0.400	16:18:53	16:18:57	00:04
PKI无法实现()				
	1	数据的完整性		
	2	数据的机密性		
+	3	权限分配		
	4	身份认证		

42 S	0.400	16:18:57	16:19:03	00:06
在对一个企业进行信息安全体系建设中，下面哪种方法是最佳的				
	1	自下而上		
+	2	自上而下		
	3	这些都不正确		
	4	上下同时开展		

43 S	0.400	16:19:01	16:19:08	00:07
在DES算法中，如果给定初始密钥k，经子密钥产生器产生的各个子密钥都相同，则称该密钥k为弱密钥，DES算法弱密钥的个数为				
+	1	4		
	2	2		
	3	8		
	4	16		

44 S	0.400	16:19:08	16:19:14	00:06
下列哪一些对信息安全漏洞的描述是错误的				
	1	具有可利用性和违规性，它本身的存在虽不会造成破坏，但是可以被攻击者利用，从而给信息系统安全带来威胁和损失		
+	2	漏洞都是人为故意引入的一种信息系统的弱点		
	3	漏洞是存在于信息系统的某种缺陷		
	4	漏洞存在于一定的环境中，寄生在一定的客体上(如TOE 中、过程中等)		

45 S	0.400	16:19:14	16:19:22	00:08
以下哪一项措施无助于防止源自内部的数据窃取行为？				
解释 解析：				
	1	数据库审计		
	2	数据加密		
	3	账户最小权限控制		
+	4	WAF防火墙		

46 S	0.400	16:19:22	16:19:26	00:04
以下不属于业务影响分析维度的是。				
	1	财务影响		
+	2	法规影响		
	3	声誉影响		
	4	运营影响		

47 S	0.000	16:19:26	16:19:28	00:02
系统定期重启在信息安全方面最重要的好处是				
	1	防止重启时出现严重故障。		
-	2	便于安装系统更新或补丁。		
	3	将系统性能维持在最佳状态。		
	4	清除不必要的垃圾数据。		

48 S	0.000	16:19:29	16:19:32	00:03
以下几种功能中，哪个是DBMS的控制功能?				
-	1	数据恢复		
	2	数据定义		
	3	数据修改		
	4	数据查询		

49 S	0.000	16:19:32	16:19:37	00:05
漏洞扫描工具由于是采用自动化匹配规则，会存在较大的误报率，有些工具报告的漏洞隐患只要采取了正确的使用方法，即使存在也				

不会造成风险。以下哪些不是可以忽略的问题		
-	1	Web服务器允许列出文件列表
	2	Debug选项没有关闭，出错时显示完整的服务器信息和堆栈信息
	3	Web服务器允许除GET、HEAD、POST以外的方法
	4	robots.txt存在未确认疑似的管理员链接

50 S	0.400	16:01:16	16:01:35	00:19
虽然公司每年进行员工信息安全意识培训，但是最近还是发生了一起因钓鱼攻击而导致的信息安全事件。以下哪些工作可以最有效提高信息安全意识的培训效果？				
	1	重新复核信息安全意识培训材料以及检查是否存在部分员工没有参加培训的情况		
+	2	定期对全体员工进行社会工程攻击测试，并将测试结果发送给员工		
	3	采购信息安全设备加强公司信息安全管控水准		
	4	对引发信息安全事件的员工进行处罚并通报全公司以儆效尤		

51 S	0.000	16:01:35	16:01:40	00:05
请回答，一批可以由攻击者进行控制远程的计算机，叫什么名字？				
	1	间谍程序		
	2	木马		
	3	僵尸网络		
-	4	肉鸡		

52 S	0.400	16:01:40	16:01:50	00:10
以下哪项措施能够最有效的降低内部攻击的风险？				
	1	对所有的员工和分包商进行全面的无犯罪记录调查		
	2	确保有一个全面完善的事件响应计划		
	3	记录关键系统的所有用户活动		
+	4	根据每个人的职责要求，限定最小的访问权限		

53 S	0.400	16:01:50	16:01:55	00:05
证书认证授权机构吊销了一个证书，可能是因为:				
	1	用户的公钥泄漏		
	2	用户搬去了一个新的城市		
	3	用户改为使用PEM信任模型来进行服务		
+	4	用户的私钥泄漏		

54 S	0.400	16:01:55	16:02:04	00:09
为了保护网页，我们将被保护的网页分类，并放置于不同的目录下，这是为了（ ）				
	1	调用方便		
	2	便于访问		
	3	便于网站的改版		
+	4	便于管理		

55 S	0.000	16:02:04	16:02:27	00:23
常见的数据模型是				
	1	逻辑模型、概念模型、关系模型		
-	2	概念模型、实体模型、关系模型		
	3	层次模型、网状模型、关系模型		
	4	对象模型、外部模型、内部模型		

56 S	0.400	16:02:27	16:02:44	00:17
网站访问被Google Chrome浏览器拦截（红底白字），提示危险网站，最快速的处理方式是				
	1	在Web服务软件上为网站配置新的监听端口，不使用默认的80端口		
	2	修改网站域名，为网站重新增加一个子域名来提供访问		
+	3	登录Google Search Console确认网站所有权之后，获取安全问题对应的网站和URL，整顿网站，申诉解禁		
	4	关闭Chrome的安全提醒，继续浏览访问		

57 S	0.400	16:02:44	16:02:47	00:03
C语言中字符型(char)数据在内存中的存储形式是				
+	1	ASCII码		
	2	反码		
	3	原码		
	4	补码		

58 S	0.000	16:02:48	16:03:13	00:25
以下哪个因素可能导致单点登录(SSO)中的单点失效？				
	1	用户的工作主机		
	2	登录凭据		
-	3	RADIUS		
	4	身份验证服务器		

59 S	0.400	16:03:13	16:03:17	00:04
下列（ ）事件中，在网页卸载时发生				
	1	Load		
+	2	Unload		
	3	Databinding		
	4	Init		

60 S	0.400	16:03:17	16:03:30	00:13
下列哪一项不是黑客在入侵踩点（信息搜集）阶段使用到的技术				
	1	主机及系统信息收集		
	2	公开信息的合理利用及分析		
	3	IP及域名信息收集		
+	4	使用sqlmap验证SQL注入漏洞是否存在		

61 S	0.400	16:03:30	16:03:51	00:21
安全管理的目标是				
	1	提高网络的容错能力		
	2	保障网络正常畅通地工作		
	3	提供用户使用网络资源的汇总与统计		
+	4	控制用户对网络敏感信息资源的使用		

62 S	0.400	16:03:51	16:03:57	00:06
以下哪一项措施可最有效地支持24*7可用性？				
	1	日常备份		
	2	异地存储		
	3	定期测试		
+	4	镜像		

63 S	0.400	16:03:58	16:04:07	00:09
以下哪一项最有可能发生在系统开发项目编码阶段的中期？				
	1	回归测试		
	2	验收测试		
+	3	单元测试		
	4	压力测试		

64 S	0.400	16:04:07	16:04:20	00:13
如何快速判定网站域名被恶意篡改？				
	1	访问网站首页面底部出现弹框广告		
	2	网站访问变慢		
+	3	网站域名解析IP发生改变，查询解析IP归属地在国外		
	4	网站出现博彩色情信息		

65 S	0.400	16:04:20	16:04:23	00:03
下列网络通信协议中，（ ）代表超文本传输协议。				
	1	ftp		
+	2	http		
	3	这些都不对		
	4	mailto		

66 S	0.400	16:04:23	16:04:48	00:25
RSA中取n=187，e=3，则d=？				
+	1	107		
	2	103		
	3	101		
	4	105		

67 S	0.400	16:04:49	16:05:00	00:11
下列服务中提供域名解析服务的是				
	1	WINS		
	2	DHCP		
+	3	DNS		
	4	WISH		

68 S	0.400	16:05:00	16:05:07	00:07
在开展系统脆弱性扫描之前，您必须				
	1	签署保密协议。		
	2	确保目标系统管理者不知情。		
+	3	活动目标系统所有者的授权。		
	4	报告直接上级。		

69 S	0.400	16:05:07	16:05:15	00:08
以下哪一项不属于数据库常用的加密方式？				
解释 解析：				
+	1	专用中间件加密		
	2	库内加密		
	3	硬件/软件加密		
	4	库外加密		

70 S	0.400	16:05:15	16:05:18	00:03
Linux 的日志文件通常保存在以下目录				
解释 解析：基本知识。				
	1	/etc/syslogd		
	2	/var/syslog		
+	3	/var/log		
	4	/etc/issue		

71 S	0.400	16:05:18	16:05:37	00:19
下面关于sql注入语句的解释，正确的是				
	1	“and 1=1”配合“and 1=2”常用来判断url中是否存在注入漏洞		
	2	and exists(select * from表名)常用来猜解表名		
+	3	都是		
	4	and exists(select字段名from表名)常用来猜解数据库表的字段名称		

72 S	0.000	16:05:37	16:06:09	00:32
下列哪个是一个安全策略成功的最重要因素？				
-	1	将安全策略集成到安全程序		
	2	将灾难恢复（DR）集成到业务连续性		
	3	将安全策略集成到业务流程		
	4	将安全意识教育集成到技术培训		

73 S	0.400	16:06:09	16:06:18	00:09
以下哪种方法不能有效提高加密的强度（）				
	1	使用公开并经过同行评审的算法		
	2	加快密钥更换的频率		
+	3	使用自己设计的秘密不公开的算法		
	4	使用更长的加密密钥		

74 S	0.400	16:06:18	16:06:28	00:10
以下漏洞中，不能直接被攻击者利用进行远程代码执行的是。				
	1	Struts2S2-016		
	2	MS08-067		
	3	Shellshock		
+	4	HeartBleed		

75 S	0.400	16:06:28	16:06:42	00:14
网络监听（嗅探）的这种攻击形式破坏了下列哪一项内容？				

	1	网络信息的完整性
+	2	网络信息的保密性
	3	网络信息的抗抵赖性
	4	网络服务的可用性

76 S	0.000	16:06:42	16:06:53	00:11

以下哪种架构不属于冯·诺伊曼架构？

	1	PPC
	2	MIPS
	3	AVR
-	4	RISC-V

77 S	0.000	16:06:53	16:07:09	00:16

身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是

	1	数字签名机制是实现身份鉴别的重要机制
	2	身份鉴别一般不用提供双向的认证
-	3	目前一般采用基于对称密钥加密或公开密钥加密的方法
	4	身份鉴别是授权控制的基础

78 S	0.400	16:07:09	16:07:39	00:30

下列哪项是一个云服务提供商保护客户数据的最佳做法？()

	1	该供应商的所有加密的客户数据与一个单一的密钥绑定
+	2	数据所有者管理密钥。
	3	强制最大密钥长度。
	4	用密钥验证数据的完整性。

79 S	0.400	16:07:39	16:07:51	00:12

某视频网站的用户帐号数据被泄露、公开，接下来的最正确做法是？

解释
解析：

	1	在朋友圈、微博转发该数据泄露新闻
	2	吐槽该视频网站的网络安全工作做的不好
	3	想法设法获取所有披露数据并存储，留着以后撞库、渗透测试使用
+	4	筛选出披露数据中使用公司/企业邮箱注册的用户，并立即通知这些用户更新邮箱密码

80 S	0.000	16:07:51	16:08:34	00:43

在自主访问控制中，谁有权限分配数据的访问权限

解释
解析:在自助访问控制者，资源的拥有者可以定义资源的访问权限，用户只能对自己拥有的资源进行权限分配，不能随意进行资源分配。

	1	用户
	2	资源的拥有者
-	3	安全管理人员
	4	安全策略

81 S	0.400	16:08:34	16:08:41	00:07

测试数据脱敏处理是为了防止

	1	生产数据发生错误。
+	2	生产数据遭到泄漏。
	3	测试数据中包含错误信息。
	4	测试数据缺乏代表性。

82 S	0.000	16:08:41	16:08:55	00:14

当针对整个页面调用（）方法时，就会计算页面上所有数据绑定表达式。

	1	DataBind()
	2	ReadXML()
-	3	DataBinder.Eval()
	4	Fill()

83 S	0.000	16:08:55	16:09:22	00:27

下列哪一项安全控制措施不是用来检测未经授权的信息处理活动的

-	1	启用时钟同步

	2	设置网络连接时限
	3	记录并分析用户和管理员操作日志
	4	记录并分析系统错误日志

84 S	0.000	16:09:22	16:09:25	00:03
以下哪个术语较好得表述了将安全相关任务的不同部分安排给不同的人来完成这种安全控制措施？				
-	1	最小授权		
	2	因需知晓		
	3	职务分离		
	4	可审核性		

85 S	0.400	16:09:25	16:09:29	00:04
char类型的长度为（ ）个字节				
	1	3		
	2	4		
	3	2		
+	4	1		

86 S	0.400	16:09:29	16:10:50	01:21
下列哪个nmap选项得不到远程主机的开放端口？				
解释 解析 2 考察对常用攻防工具的掌握				
+	1	-sP		
	2	-A		
	3	-sV		
	4	-PS		

87 S	0.400	16:09:55	16:09:57	00:02
请问以下哪一种安全门是不可以从外进入机房的？				
	1	主用门		
	2	备用门		
+	3	应急门		
	4	货物门		

88 S	0.400	16:09:57	16:11:04	01:07
以下何种安全机制对于穷举式的登录攻击有最好的防范效果？				
	1	禁止通过电子邮件发送初始口令		
	2	更改系统中的默认和简单口令		
+	3	引入失败登录后暂缓登录机制		
	4	降低用户同时在线会话限额		

89 S	0.400	16:11:04	16:11:18	00:14
数据库的运行管理与维护主要由数据库管理员负责，工作内容主要包括日常维护、系统监控与分析、性能优化等。下列关于数据库管理员工作内容的说法错误的是				
	1	数据库管理员需要定期检查存储空间使用情况并根据需求扩展存储空间，这些工作一般无需最终用户参与		
	2	数据库管理员应监控数据库中各种锁的使用情况，并处理可能出现的死锁情况，若发现问题应及时通知相关人员		
	3	数据库的备份和恢复是重要的维护工作，数据库管理员应根据不同的应用要求制定不同的备份计划，在备份计划中应包含备份的时间、周期、备份方式和备份内容等		
+	4	性能优化是数据库管理员的重要工作，性能优化的主要手段有查询优化、索引调整、模式调整等，这些工作一般无需开发人员参与		

90 S	0.400	16:11:18	16:11:23	00:05
某网站安全防护措施得当，近期也没有发现安全入侵事件，但是网上流传出一份该网站的用户名密码列表，经过尝试确实可以登陆。经过安全人员排查，得出这是一起“撞库”事件。请问，下列措施中无法减少撞库攻击的是				
+	1	存储用户密码时使用2次MD5		
	2	注册时提醒用户避免使用和其他网站相同的密码		
	3	用户登陆时增加双因子认证		
	4	存储用户密码时加上随机字符串		

91 S	0.400	16:11:23	16:11:32	00:09
以下哪项不是防范慢速HTTP（SlowHTTP）拒绝服务（DoS）攻击的有效手段？				
	1	在Web服务器上设置每个IP可以向其发起的最大连接数		
	2	在Web服务器上设置接收请求主体（body）超时时间		

	3	在Web服务器上设置接收请求头部（header）超时时间
+	4	在Web服务器上设置连接超时时间

92 S	0.400		16:11:32	16:11:51	00:19
针对网站发现的身份证号码泄露问题应急处理，下面哪一项操作是错误？					
	1	撤稿存在身份证号码的文章			
	2	对搜索引擎中包含身份证号码的快照进行投诉，申请刷新			
+	3	修改存在身份证号码文章中的学生姓名，将汉字统一成拼音，干扰识别			
	4	删除网站中存在身份证号码的附件文件（xls doc）			

93 S	0.000		16:11:52	16:12:12	00:20
下列哪种隐藏属于文本的语义隐藏					
	1	对文本的字、行、段等位置做少量修改			
-	2	修改文字的字体来隐藏信息			
	3	根据文字表达的多样性进行同义词置换			
	4	在文件头、尾嵌入数据			

94 S	0.000		16:12:12	16:12:30	00:18
下列哪个是信息所有者的主要责任？					
	1	审核数据的准确度以及当前对这些信息资产相关的访问权限情况			
	2	提供数据安全设计的输入、咨询和评审			
-	3	检查和验证访问权限的请求是否与安全政策和指导方针一致			
	4	审查和核实数据的准确性			

95 S	0.000		16:12:30	16:12:49	00:19
下面哪一种说法的顺序正确？					
	1	威胁导致了脆弱性，然后脆弱性导致了风险			
-	2	脆弱性导致了风险，然后风险导致了威胁			
	3	风险导致了威胁，然后威胁导致了脆弱性			
	4	脆弱性导致了威胁，然后威胁导致了风险			

96 S	0.400		16:12:49	16:12:51	00:02
Linux系统/etc目录从功能上看相当于Windows的哪个目录？					
	1	program files			
+	2	Windows			
	3	system volume information			
	4	TEMP			

97 S	0.400		16:12:51	16:12:57	00:06
请问以下哪一种装置可以吸收过剩电流，阻止其流向电子设备？					
+	1	浪涌保护器			
	2	备用电源			
	3	恒压变压器			
	4	接地装置			

98 S	0.000		16:12:57	16:13:47	00:50
数据主体对于将被收集的隐私数据应在事先享有知情权，使用过程中享有访问权、修正权、被遗忘权、限制使用权及携带权，事后享有____？					
解释 解析：					
-	1	数字权			
	2	专利权			
	3	拒绝权			
	4	买卖权			

99 S	0.400		16:13:48	16:20:53	07:05
《中华人民共和国网络安全法》中规定，使用未经安全审查或者安全审查未通过的网络 产品或者服务的，应处以何种处罚？					
	1	处采购 金额一倍以上五倍以下罚款；对直接负责的主管人员和其 他直接责任人员处一万元以上十万元以下罚款。			
	2	处采购 金额一倍以上十倍以下罚款；对直接负责的主管人员和其 他直接责任人员处五千元以上五万元以下罚款。			
+	3	处采购 金额一倍以上十倍以下罚款；对直接负责的主管人员和其 他直接责任人员处一万元以上十万元以下罚款。			
	4	处采购 金额一倍以上五倍以下罚款；对直接负责的主管人员和其 他直接责任人员处五千元以上五万元以下罚款。			

100 S	0.400		14:26:59	16:20:56	53:57

以下哪种加密算法是基于Feistel结构？		
	1	RSA
	2	AES
	3	RC4
+	4	DES

101 S	0.000	14:27:17	14:30:16	02:59
安全监控中心一般不能解决以下哪种问题？				
	1	不能及时发现攻击源		
	2	设备日志格式各异，难以检索		
	3	很难将安全威胁可视化呈现		
-	4	业务系统过多，资产难以迅速定位		

102 S	0.400	14:30:17	14:31:20	01:03
从技术角度上看数据安全的技术特征主要包含哪几个方面？				
	1	数据的方便性、数据的稳定性、数据的完整性		
+	2	数据的完整性、数据的保密性、数据的可用性		
	3	数据的稳定性、数据的保密性、数据的可用性		
	4	数据完整性、数据的方便性、数据的可用性		

103 S	0.400	14:31:20	14:32:27	01:07
下面哪种密码算法抵抗频率分析攻击能力最强，而对已知明文攻击最弱				
	1	维吉利亚		
	2	轮转密码		
+	3	希尔密码		
	4	仿射密码		

104 S	0.000	14:32:27	14:37:03	04:36
以下哪一项不是动态分析调试技术的优点？				
	1	执行速度较快、效率高		
	2	无需访问软件真正的源代码		
-	3	支持跟踪软件中可能引起安全混乱的细微逻辑错误		
	4	无需创建认为导致错误的场景		

105 S	0.400	14:37:03	14:37:15	00:12
下面关于IIS报错信息含义的描述正确的是				
	1	404-权限问题		
+	2	403-禁止访问		
	3	500-系统错误		
	4	401-找不到文件		

106 S	0.000	14:37:15	14:37:31	00:16
DNS 系统对于网络服务是至关重要的，以下措施中不能增强DNS 安全性的是				
解释 解析：更改端口号会导致默认设置的客户端无法使用DNS				
-	1	隐藏服务器版本标识		
	2	更改DNS的端口号		
	3	使用防火墙控制对DNS 的访问		
	4	限制区域传输		

107 S	0.400	14:37:31	14:37:55	00:24
维吉利亚(Vigenere)密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是				
	1	序列密码		
+	2	多表代换密码		
	3	单表代换密码		
	4	置换密码		

108 S	0.400	14:37:55	14:39:22	01:27
通过对称密码算法进行安全消息传输的必要条件是				
+	1	通讯双方通过某种方式，安全且秘密地共享密钥		
	2	通讯双方将传输的信息夹杂在无用信息中传输并提取		
	3	在安全的传输信道上进行通信		
	4	通讯双方使用不公开的加密算法		

109 S	0.400	14:39:22	14:40:31	01:09
一个组织的灾难恢复计划中对于某关键信息系统的恢复时间目标（RTO）设定为一分钟，恢复点目标（RPO）设定为两分钟，以下哪项关于系统灾难恢复的描述正确？				
	1	确保系统数据丢失在一分钟内的处理措施都是适用的		
	2	确保系统在两分钟内恢复运行的处理措施都是适用的		
+	3	数据丢失不超过两分钟，系统中断间隔不超过一分钟		
	4	一分钟前的数据需全部恢复，两分钟内系统恢复运行		

110 S	0.400	14:40:31	14:40:46	00:15
不同厂商所生产的IDS系统其日志格式可能不同，但具有通用的通信格式，请问该格式是				
	1	IETF		
	2	IEEE		
+	3	IDMEF		
	4	IEGF		

111 S	0.400	14:40:46	14:41:25	00:39
AES密钥长度不可能是多少bit？				
+	1	224		
	2	128		
	3	192		
	4	256		

112 S	0.400	14:41:25	14:48:13	06:48
以下哪项措施可以有效防止内部用户非授权修改信息？				
	1	建立数据安全标准		
	2	定期检查系统中的异常操作日志		
+	3	建立基于角色的访问控制措施		
	4	定义明确的数据所有者信息		

113 S	0.400	14:48:13	14:48:40	00:27
关系数据库中的投影操作是指从关系中				
	1	抽出特定记录		
	2	建立相应的影像		
	3	建立相应的图形		
+	4	抽出特定字段		

114 S	0.400	14:48:40	14:53:25	04:45
“进不来”、“拿不走”、“看不懂”、“改不了”、“走不脱”是网络信息安全建设的目的。其中，“拿不走”主要使用下面哪种安全技术。				
	1	身份认证		
+	2	访问控制		
	3	数据加密		
	4	数据完整性		

115 S	0.400	14:53:25	14:53:52	00:27
涉及国家秘密的计算机信息系统，必须。				
	1	实行单向隔离		
+	2	实行物理隔离		
	3	在重要时期进行隔离		
	4	实行逻辑隔离		

116 S	0.400	14:53:52	14:53:59	00:07
反映现实世界中实体及实体间联系的信息模型是				
+	1	E-R模型		
	2	网状模型		
	3	层次模型		
	4	关系模型		

117 S	0.400	14:53:59	16:21:32	27:33
HTTPS是在SSL上运行的HTTP，为浏览器和服务器之间的通信提供了服务器端身份验证，完整性保护和数据加密等多项服务功能，下列那项关于SSL运行过程的描述是错误的：				
+	1	SSL数据传输过程中加密数据使用的是服务端的私钥		
	2	SSL通信开始时，浏览器和服务器双方要交换安全参数，确定要采用的协议版本等信息		
	3	SSL通信过程中服务器端要向浏览器提供自己的证书，供浏览器验证服务器的身份		

	4	SSL在协议握手阶段后，所有的信息都是加密传输的	

118 S	0.400	15:00:28	16:21:27	20:59
Oracle、MSSQL、MySQL三种数据库，最高权限的用户分别是				
解释 解析：基本概念				
	1	root、sa、sys		
	2	dbsnmp、sa、root		
	3	sys、root、sa		
+	4	sys、sa、root		

119 S	0.400	15:01:04	15:01:38	00:34
下面哪个符号不能用于命令截断				
	1	;		
	2	%0a		
	3	|		
+	4	,		

120 S	0.400	15:01:38	15:01:53	00:15
一个网站采用了防火墙、入侵检测（IDS）和防病毒系统。但怀疑可能发生了针对用户帐户的欺诈活动。如何确认欺诈的发生？				
+	1	在Web应用程序中部署日志		
	2	确保Web服务器的补丁是最新的		
	3	对所有用户实施强身份认证		
	4	定期审查防火墙日志		

121 S	0.400	15:01:53	15:01:56	00:03
下面哪个php函数可能造成变量覆盖				
+	1	extract		
	2	strpos		
	3	strcmp		
	4	in_array		

122 S	0.000	15:01:56	15:02:43	00:47
下面哪一种方法在保护系统免受非授权人员的访问时可以提供最高级安全？				
-	1	用户身份别码和口令		
	2	加密		
	3	电话回叫或拨号回叫系统		
	4	含有个人身份识别码的磁卡		

123 S	0.000	15:02:43	15:03:16	00:33
将不受信任的数据作为命令或查询的一部分发送到解析器时，会产生诸如SQL注入、NoSQL注入、OS注入和LDAP注入的注入缺陷。其中SQL注入漏洞最正确的预防措施是				
	1	过滤和转义单引号、双引号和他们的所有变种		
	2	使用参数化查询		
-	3	在Web后台部署注入防火墙，通过AI自学习常用的SQL语句建立白名单，对于白名单以外的查询不响应并记录		
	4	对输入的变量使用黑名单机制检测包括但不止于DELETE、UPDATE		

124 S	0.000	15:03:16	15:03:58	00:42
信息化建设和网络安全建设的关系应该是				
	1	信息化建设的结果就是信息安全建设的开始		
-	2	信息化建设和信息安全建设应同步规划、同步实施		
	3	这些说法都正确		
	4	信息化建设和信息安全建设是交替进行的，无法区分谁先谁后		

125 S	0.000	15:03:41	15:04:13	00:32
下列哪个是实施信息安全等级保护的最重要的原因？				
	1	简化数据管理程序		
	2	提高投资回报率（ROI）		
	3	改进业务流程		
-	4	增强资产保护		

126 S	0.400	15:04:13	15:04:48	00:35
以下关于变更控制措施，错误的是？				

+	1	重要的变更在变更后应准备回退方案，并确保切实可行
	2	对涉及到内部管理系统的重大生产变更，变更前应通知相关部门，对有可能影响客户利益的变更，应事先进行公告
	3	所有变更申请都应经过授权或审批
	4	应保留所有与变更相关信息的日志

127 S	0.000	15:04:48	15:06:54	02:06
以下关于TLS 1.3的说法，哪个是错误的？				
	1	加密了SNI域名		
	2	支持0-RTT		
-	3	加密了服务器证书		
	4	不再支持MD5		

128 S	0.400	15:06:54	15:07:15	00:21
代码签名的目的是确保：				
	1	应用（程序）的签名人是受到信任的		
	2	应用程序可以与其它已签名的应用安全地对接使用		
+	3	软件没有被后续修改		
	4	签名人的私钥还没有被泄露		

129 S	0.400	15:07:15	15:07:34	00:19
以下哪项可以最有效评估员工信息安全意识培训效果？				
	1	针对安全培训的满意度调查结果		
+	2	模拟钓鱼攻击测试结果		
	3	培训出席率		
	4	培训后安全考试成绩		

130 S	0.400	15:07:34	15:07:40	00:06
Linux的防火墙包括几个不同的访问控制表来执行不同的功能，其中缺省的控制表是：				
	1	NAT		
+	2	FILTER		
	3	MANGLE		
	4	RAW		

131 S	0.400	15:07:40	16:21:44	14:04
假设已完成了一个注册界面，包括用户名、密码、身份证三项注册信息，并为每个控件设置了必须输入的验证控件。但为了测试的需要，暂时取消该页面的验证功能，该如何做				
	1	将相关的验证控件属性ControlToValidation属性设置为false		
	2	将提交按钮的CausesValidation属性设置为true		
+	3	将提交按钮的CausesValidation属性设置为false		
	4	将相关的验证控件属性ControlToValidation属性设置为true		

132 S	0.400	15:09:16	15:10:00	00:44
关于F5算法隐写过的JPEG图像，下列哪种说法不正确				
	1	DCT变换以小块为基本单位，高通滤波后，隐写图像小块间的不连续性更加明显。		
+	2	观察隐写图像的灰度直方图可以发现值对频度趋于相等。		
	3	隐写图像的DCT量化系数直方图不会出现偶数位置色柱比奇数位置色柱更突出的现象。		
	4	与原始图像相比，隐写图像的DCT量化系数直方图更“瘦”、更“高”。		

133 S	0.400	15:10:00	15:10:25	00:25
在漏洞挖掘领域，下列哪个技术不是直接用于分析输入数据对程序行为的影响？				
解释 解析: 4 考察对常见漏洞挖掘技术的理解				
	1	污点分析		
	2	模糊测试		
	3	符号执行		
+	4	PATCH比较		

134 S	0.400	15:10:25	15:10:31	00:06
字母频率分析法对下面哪种密码算法最有效				
	1	序列密码		
	2	多表代换密码		
	3	置换密码		
+	4	单表代换密码		

135 S	0.000	15:10:31	15:11:24	00:53
以下哪种防御方式能较为有效地防御ROP？				
-	1	NX		
	2	ASLR		
	3	PIE		
	4	RELRO		

136 S	0.000	15:11:24	15:12:07	00:43
以下哪个是恶意代码采用的隐藏技术：				
	1	都是		
	2	文件隐藏		
	3	网络连接隐藏		
-	4	进程隐藏		

137 S	0.000	15:12:07	15:14:34	02:27
系统运行期间，需定期对系统进行哪种备份？				
	1	系统级		
	2	系统级和数据级		
	3	系统级和应用级		
-	4	应用级和数据级		

138 S	0.400	15:14:34	15:14:40	00:06
下列哪一项不属于个人隐私信息？				
+	1	个人工作单位电子邮箱		
	2	个人短信和通话记录		
	3	手机通讯录信息		
	4	个人自拍照片和视频		

139 S	0.000	15:14:40	15:15:08	00:28
在数据库应用系统的需求分析阶段，需要考虑数据的安全性需求。下列不属于数据安全性需求分析内容的是				
	1	分析数据的安全性需求，以确定每个关系表上定义的数据约束能够满足使用要求		
	2	分析全局用户对数据的存取需求，以确定全局数据的安全控制策略		
-	3	分析各类用户对数据的存取需求，以确定各类用户能够操作的数据		
	4	分析特殊用户对数据的存取需求，以保证数据库的安全控制策略能够满足其使用要求		

140 S	0.400	15:15:08	15:16:29	01:21
Snort是一种Linux系统下的轻量级入侵检测系统，请问下面哪项不属于其工作模式				
解释 解析：snort三种工作模式:1. 嗅探 (snort从网络上读出数据包并将其显示在控制台上）;2. 数据包记录器（将数据包记录在硬盘上）;3. NIDS（最复杂，可配置，允许snort匹配用户自定义的数据集，并根据检测结果执行一定的动作）				
+	1	主机入侵检测系统		
	2	嗅探器		
	3	数据包记录器		
	4	网络入侵检测系统		

141 S	0.000	15:16:29	15:16:49	00:20
从风险分析的观点来看，计算机系统的最主要弱点是				
-	1	通讯和网络		
	2	外部计算机处理		
	3	系统输入输出		
	4	内部计算机处理		

142 S	0.400	15:16:49	15:16:52	00:03
glibc的堆管理机制中，默认情况下fastbin的堆块大小不大于？				
	1	0x70		
	2	0x90		
	3	0x60		
+	4	0x80		

143 S	0.400	15:16:52	15:17:03	00:11
SHODAN是一种专用搜索Internet上漏洞的搜索引擎，关于SHODAN可以搜索的对象，下列说法正确的是：				
	1	互联网上的无线路由器		

	2	互联网上的摄像头
	3	互联网上的特定类型数据库服务器
+	4	皆是

144 S	0.400	15:17:03	15:18:27	01:24

下面关于信息安全保障的说法正确的是

	1	信息安全保障的概念是与信息安全的概念同时产生的
+	2	信息安全保障是以业务目标的实现为最终目的，从风险和策略出发，实施各种保障要素，在系统的生命周期内确保信息的安全属性
	3	信息安全保障和信息安全技术并列构成实现信息安全的两大主要手段
	4	信息系统安全保障要素包括信息的完整性、可用性和保密性

145 S	0.400	15:18:27	15:19:09	00:42

一般数据保护条例（General Data Protection Regulation）于什么时候开始在欧盟全面实施？

解释
解析：

+	1	2018年5月25日
	2	2019年1月1日
	3	2017年7月1日
	4	2016年10月1日

146 S	0.400	15:19:09	15:19:23	00:14

用户在使用应用系统之前首先要执行身份识别协议，而这个协议一般应满足

+	1	零知识证明
	2	不经意传输
	3	比特承诺
	4	安全多方计算

147 S	0.400	15:19:23	15:19:41	00:18

OpenSSH的加固措施，下列哪一项是不正确的？

+	1	编辑etc/sysconfig/i18n，增加GB2312编码语言
	2	程序更新至最新版本，如7.9sp1
	3	为远程用户配置符合密码强度的密码
	4	使用IP地址白名单限制远程连接

148 S	0.000	15:19:41	15:20:58	01:17

下面哪一个测试的错误将会为实施新的应用软件带来最大的风险？

	1	验收测试
	2	整合测试
-	3	系统测试
	4	单元测试

149 S	0.400	15:20:58	15:21:27	00:29

下面关于入侵检测（IDS）系统的说法，错误的是

解释
解析：基于主机的HIDS不一定需要检测网络行为即可发现异常。

	1	假如说防火墙是一幢大楼的门锁，那么IDS就是这幢大楼里的监视系统
	2	IDS报警存在误报和漏报问题
	3	IDS只能够检测并发现异常，并不能阻止异常
+	4	IDS必须通过监控网络行为才能够发现异常行为

150 S	0.400	15:21:27	15:21:52	00:25

概念模型是现实世界的第一层抽象，这一类模型

	1	网状模型
	2	关系模型
	3	层次模型
+	4	实体-关系模型

151 S	0.400	15:21:52	15:22:06	00:14

下列除了（ ）以外，都是防范计算机病毒侵害的有效方法

+	1	机房保持卫生，经常进行消毒
	2	谨慎使用外来的移动介质
	3	网络使用防病毒网关设备

	4	使用防病毒软件	

152 S	0.400	15:22:06	15:25:02	02:56
SIEM产品的功能一般不包含下面哪一项？				
	1	报警以及事件升级		
	2	及时监控		
+	3	网络设备配置管理		
	4	网络分析		

153 S	0.400	15:25:02	15:25:40	00:38
以下关于对称密钥加密说法正确的是				
	1	加密密钥和解密密钥可以是不同的		
+	2	加密密钥和解密密钥必须是相同的		
	3	密钥的管理非常简单		
	4	加密方和解密可以使用不同的算法		

154 S	0.400	15:25:40	15:25:57	00:17
以下哪一项不是用于提升邮件安全的协议？				
解释 解析：				
	1	DMARC		
	2	SPF		
+	3	IMAP		
	4	DKIM		

155 S	0.000	15:25:57	15:26:18	00:21
Apache Httponly Cookie泄露漏洞，正确的处理方法是				
	1	Apache关闭Httponly，取消LimitRequestFieldSize 的长度		
	2	网站为Cookie信息内容使用强加密算法		
-	3	为Apache配置HTTP 400错误的跳转页面		
	4	升级Apache到2.2.21以上版本		

156 S	0.400	15:26:18	15:26:23	00:05
_____负责统筹协调网络安全工作和相关监督管理工作				
	1	公安部门		
+	2	国家网信部门		
	3	国务院电信主管部门		
	4	这些均是		

157 S	0.400	15:26:23	15:27:08	00:45
下面对Oracle的密码规则描述，哪个是错误的？				
	1	Oracle密码必须由英文字母，数值，#，下划线(_)，美元字符（$）构成，密码的最大长度为30字符，并不能以“$”，“#”，“_”或任何数字卡头；密码不能包含像“SELECT”，“DELETE”，“CREATE”这类的ORACLE/SQL关键字		
+	2	密码长度没有限制		
	3	Oracle默认配置下，用户如果大量失败登录，此账户将会被锁定		
	4	Oracle的若算法加密机制（ ）两个相同的用户名和密码在两台不同的ORACLE数据库机器中，将具有相同的哈希值。这些哈希值存储在SYS.USER表中，可以通过像DBA_USE这类的试图来访问		

158 S	0.400	15:27:08	15:27:12	00:04
内容安全策略（Content Security Policy，CSP）的实质就是白名单制度，即使网站代码存在某些漏洞，攻击者也无法进行有效的攻击，CSP可以预防下面哪个问题				
	1	SSRf		
	2	CSRF		
+	3	XSS		
	4	XXE		

159 S	0.400	15:27:12	15:27:38	00:26
组织通过部署安全信息和事件管理系统（SIEM）来集中处理各类安全信息和事件，SIEM能够统一处理不同安全系统产生的信息和事件的重要机制是：				
	1	虚拟化网络		
+	2	信息标准化		
	3	机器学习		
	4	分布式存储		

160 S	0.000	15:27:38	15:27:41	00:03
Metasploit是近年来出现的一种免费的可视化漏洞远程利用工具。该工具自带数百种漏洞利用程序，并可方便地增加自己的漏洞利用程序。这反映出当前的攻击技术呈现出趋势。				
	1	平台化		
	2	组织化		
	3	趋利化		
-	4	简单化		

161 S	0.400	15:27:41	15:27:57	00:16
要保证数据库的数据独立性，需要修改的是				
+	1	三级模式之间的两层映射		
	2	模式与内模式		
	3	三层模式		
	4	模式与外模式		

162 S	0.400	15:27:57	15:28:10	00:13
请问通常webshell功能不包括以下哪项内容				
解释 解析：webshell被常常用于网站管理、服务器管理等等，根据FSO权限的不同，作用有在线编辑网页脚本、上传下载文件、查看数据库、执行任意程序命令等。				
	1	文件上传下载		
+	2	拦截网络流量		
	3	查看数据库		
	4	执行程序命令		

163 S	0.400	15:28:10	15:28:44	00:34
（）方法用于写文本响应以回应对网页的请求				
	1	TextWrite		
+	2	Write		
	3	Read		
	4	Rewrite		

164 S	0.400	15:28:44	15:28:49	00:05
以下哪个不是二维码的优点？				
	1	成本低，易制作，持久耐用		
	2	容错能力强，具有纠错功能		
	3	编码范围广，译码可靠性高		
+	4	加密措施强，可作为认证机制		

165 S	0.000	15:28:49	15:29:01	00:12
对保护数据来说，哪种软件更为重要？				
-	1	网络软件		
	2	数据库软件		
	3	备份软件		
	4	系统软件		

166 S	0.400	15:29:01	15:29:19	00:18
以下哪一项攻击方法最符合社会工程的定义？				
	1	通过搜寻垃圾箱等废弃资料收集敏感信息		
	2	通过网络嗅探截获敏感信息		
	3	偷看用户输入敏感信息		
+	4	利用人的弱点获得敏感信息		

167 S	0.400	15:29:19	15:29:36	00:17
在部署HTTPS时，为了安全我们会考虑HSTS（HTTP Strict-Transport-Security），HSTS会强制客户端使用HTTPS访问页面，以下哪种不是HSTS的实现方法				
	1	STS-in-DNS，在DNS条目内强制要求对域名使用TLS访问		
+	2	STS-over-TCP，在TCP底层协议上升级要求TLS访问		
	3	使用浏览器的HSTS Preload List，预置域名列表		
	4	在Response Header写Strict-Transport-Security		

168 S	0.400	15:29:36	15:29:51	00:15
完整性检查和控制的防范对象是_____，防止它们进入数据库				

+	1	不合语义的数据，不正确的数据
	2	非法授权
	3	非法用户
	4	非法操作

169 S	0.400	15:29:51	15:30:20	00:29

利用IE浏览器0day漏洞，攻击者将恶意代码嵌入正常的Web页面当中，用户访问URL之后会自动下载并运行木马程序，这种攻击从技术原理上属于

解释

解析：3 考察浏览器漏洞攻击的基本概念和原理

	1	网页劫持
+	2	网页挂马
	3	网页木马
	4	网站钓鱼

170 S	0.400	15:30:20	15:31:24	01:04

A方和B方均拥有数字证书，但是不是同一个CA机构颁发的，为了使两个证书之间建立起可信任的相互依赖关系，可以采用以下哪种方法？

	1	证书链校验
+	2	交叉认证
	3	IP认证
	4	CA认证

171 S	0.400	15:31:24	15:31:32	00:08

1949 年，（ ）发表了题为《保密系统的通信理论》的文章，为密码技术的研究奠定了理论基础，由此密码学成了一门科学。

	1	Diffie
+	2	Shannon
	3	Shamir
	4	Hellman

172 S	0.400	15:31:32	15:31:44	00:12

以下哪项是对抗 ARP 欺骗有效的手段

	1	使用 Linux 系统提高安全性
	2	在网络上阻止 ARP 报文的发送
+	3	使用静态的 ARP 缓存
	4	安装杀毒软件并更新到最新的病毒库

173 S	0.400	15:31:44	15:31:51	00:07

STARTTLS Everywhere旨在推进：

	1	FTP协议淘汰
	2	网站HTTPS支持
+	3	邮件安全传输
	4	浏览器HTTPS支持

174 S	0.400	15:31:51	15:32:30	00:39

下面哪项不属于防火墙的主要技术

解释

解析：防火墙不提供路由交换功能。

+	1	路由交换技术
	2	状态检测包过滤技术
	3	应用代理技术
	4	简单包过滤技术

175 S	0.400	15:32:30	15:32:39	00:09

以下哪种加密模式安全性最弱？

+	1	ECB
	2	CBC
	3	CFB
	4	OFB

176 S	0.400	15:32:39	15:33:44	01:05

以下哪项不属于造成操作系统安全漏洞的原因是

+	1	人为的恶意破坏

	2	考虑不周的架构设计
	3	不安全的编程语言
	4	不安全的编程习惯

177 S	0.400	15:33:45	15:33:50	00:05
在渗透测试中，有时需要通过工具向被测应用输入大量随机或半随机的数据，通过观察被测系统的响应状况来发掘潜在的安全问题，这种方法被称为。				
+	1	模糊测试（fuzztesting）		
	2	爬取（crawling）		
	3	暴力攻击（bruteforceattack）		
	4	发现测试（discoverytest）		

178 S	0.400	15:33:50	15:34:17	00:27
以下哪种技术手段可以屏蔽网络中未经认证的DHCP客户端？				
+	1	DHCPsnooping		
	2	DHCPshielding		
	3	DHCPcaching		
	4	DHCPprotection		

179 S	0.400	15:34:18	15:34:30	00:12
信息系统验收时进行安全评估的最主要目的是：。				
	1	发现系统安全现状与相应安全等级的差异；		
	2	发现信息系统的代码层安全隐患。		
	3	发现信息系统的抗攻击能力。		
+	4	发现系统安全现状与建设之初安全目标的符合程度；		

180 S	0.400	15:34:30	15:34:44	00:14
版本控制系统是一种记录一个或若干文件内容变化，以便将来查阅特定版本修订情况的系统。我们较为常用的源代码版本控制系统是Git，以下哪个不是使用Git的正确操作				
	1	在线上系统出现安全缺陷需要紧急修复时开启了patch分支，开发完合并到主分支发布后删除patch分支		
	2	要求项目组成员经常性检查Git客户端的安全性，以避免类似CVE-2018-11235的通过恶意 .gitmodules 达到执行恶意代码的漏洞		
+	3	规范密码生成、分享和定期修改机制，将项目相关的服务器登录密码，数据库密码，管理员密码明文保存到Git，以便检查密码复杂度，在项目组内部成员内共享，并跟踪是否有定期修改密码。		
	4	为回溯某个安全缺陷代码的编写者和编写的时间，通过git log和git diff查找日志和比较文件变化情况		

181 S	0.400	15:34:44	15:34:50	00:06
“TCP SYN Flooding”建立大量处于半连接状态的TCP连接，其攻击目标是网络的				
解释 解析：这是DOS攻击，目标是可用性				
+	1	可用性		
	2	保密性		
	3	真实性		
	4	完整性		

182 S	0.400	15:34:51	15:35:24	00:33
信息安全管理中常用戴明环模型（PDCA模型），其中P、D. C. A四个字母是以下哪组单词的缩写				
解释 解析：基本概念				
	1	Policy、Do、Control、Act 策略、实施、控制、行动		
+	2	Plan、Do、Check、Act 计划、实施、检查、行动		
	3	Plan、Do、Control、Act 计划、实施、控制、行动		
	4	Protect、Do、Check、Act保护、实施、检查、行动		

183 S	0.400	15:35:24	15:35:33	00:09
在下面的选项中，不能作为函数的返回值类型的是				
	1	int		
	2	long		
+	3	node		
	4	void		

184 S	0.400	15:35:33	15:35:54	00:21
以下哪一项不是风险评估阶段应该做的？				

	1	对信息资产面对的各种威胁和脆弱性进行评估
	2	对已存在的或规划的安全控制措施进行界定
+	3	根据评估结果实施相应的安全控制措施
	4	对信息安全管理体系范围内的信息资产进行鉴定和估价

185 S	0.400	15:35:54	15:36:18	00:24
下面哪个mysql函数能用于时间盲注				
	1	mid		
	2	union		
	3	if		
+	4	benchmark		

186 S	0.400	15:36:18	15:36:59	00:41
关于HTTP与HTTPS的描述，下列哪一项是错误的？				
	1	HTTPS协议需要到CA机构申请SSL证书，免费证书较少，多数SSL证书需要一定的年费		
	2	HTTP连接很简单，是无状态的，HTTPS协议是由SSL+HTTP协议构建加密传输的网络协议		
+	3	HTTP是超文本传输协议，信息是明文传输，如果网站应用将信息使用强加密算法加密之后，与HTTPS的效果一致		
	4	HTTP和HTTPS使用的是完全不同的连接方式，使用的默认端口也不一样，HTTP是80，HTTPS是443		

187 S	0.000	15:36:59	15:37:09	00:10
下列哪个最好的描述了信息安全策略文件的基本组成部分？				
-	1	保密性，完整性，可用性，可审计性		
	2	目的，范围，职责，符合性		
	3	规划，设计，实施，管理		
	4	访问控制，病毒防护，问责，安全意识		

188 S	0.000	15:37:09	15:37:36	00:27
信息系统的保护等级取决于				
	1	信息的价值和技术的先进性。		
	2	信息的价值和运行环境的复杂程度。		
-	3	信息系统的成本和运行环境的复杂程度。		
	4	信息系统的成本及其技术的先进性。		

189 S	0.400	15:37:36	15:37:48	00:12
公司没有定期开展员工信息安全意识培训最大的风险是什么？				
	1	影响员工绩效考核结果		
+	2	增加因员工意识薄弱而发生安全事件可能性		
	3	员工无法了解公司信息安全制度要求		
	4	增加员工违反公司信息安全制度的可能性		

190 S	0.400	15:37:48	15:37:52	00:04
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				
	1	401		
+	2	404		
	3	200		
	4	302		

191 S	0.400	15:37:52	15:38:25	00:33
下面哪个是一种架构在公用通信基础设施上的专用数据通信网络，利用IPSec等网络层安全协议和建立在PKI的加密与签名技术来获得私有性。				
	1	PKIX		
+	2	VPN		
	3	DDN		
	4	SET		

192 S	0.400	15:38:25	15:39:12	00:47
为了是信息安全策略有效，下列哪个是主要的考虑因素？				
	1	技术，研究，法规		
+	2	人，流程，技术		
	3	财务，执行，标准		
	4	技术，法规，法律		

193 S	0.400	15:39:13	15:39:29	00:16

对于安全管理人员来说风险分析的最主要目的是		
	1	获得管理层的理解和支持。
	2	确定有能力的分析人员。
	3	确定自动化的分析工具。
+	4	确定最有效的防范措施。

194 S	0.400	15:39:29	15:39:44	00:15
下面哪一种属于网络上的被动攻击？				
	1	拒绝服务		
	2	消息篡改		
	3	伪装		
+	4	流量分析		

195 S	0.400	15:39:44	15:39:48	00:04
以下哪个加密算法基于一个大数很难被分解为两个质数的乘积这一问题				
解释 解析：RSA算法的原理是大数分解问题。				
	1	DES		
	2	Diffie-Hellman		
+	3	RSA		
	4	ECC		

196 S	0.400	15:39:48	15:40:34	00:46
关于域名使用期限的描述，下列哪一项是正确的？				
+	1	域名到期后不续费，可能会被注销删除，其他人可以重新申请注册		
	2	域名在正确解析的期间需要付费，如不使用则无需支付费用		
	3	域名一次注册终生拥有，因此需要保存好域名注册的邮箱和密码		
	4	COM的国际域名最长续费年限是20年，CN域名最长续费年限是5年		

197 S	0.400	15:40:34	15:41:18	00:44
DNS服务采用（ ）编码识别方式				
	1	UTF-32		
	2	UTF-64		
	3	UTF-16		
+	4	UTF-8		

198 S	0.400	15:41:18	15:41:27	00:09
下面哪个信息收集工具可以用于收集调查单位的技术联系人的姓名和地址信息：				
	1	dig		
	2	traceroute		
	3	nslookup		
+	4	whois		

199 S	0.400	15:41:27	15:41:57	00:30
可以使用图片来当作按钮的控件是				
	1	Button		
+	2	ImageButton		
	3	LinkButton		
	4	Image		

200 S	0.400	15:41:58	15:42:13	00:15
SQL Server采用的身份验证模式有（ ）				
	1	仅SQL Server身份验证模式		
+	2	Windows身份验证模式和混合模式		
	3	仅混合模式		
	4	仅Windows身份验证模式		

201 S	0.400	15:42:13	15:42:21	00:08
判断网站外链域名是否是黑链的基本依据，下列哪一项是错误的？				
+	1	外链域名注册邮箱是个人QQ邮箱		
	2	外链域名对应站点页面访问出现博彩色情内容		
	3	外链域名解析IP频繁改变，且归属地在国外		
	4	搜索引擎检索外链域名结果有“危险”提示		

202 S	0.400	15:42:21	15:42:26	00:05
为了应对日益严重的垃圾邮件问题，人们设计和应用了各种垃圾邮件过滤机制，以下哪一项是耗费计算资源最多的一种垃圾邮件过滤机？				
	1	SMTP身份认证		
+	2	内容过滤		
	3	黑名单过滤		
	4	SPF		

203 S	0.400	15:42:26	15:43:23	00:57
以下对信息安全管理体系描述最为确切的是。				
	1	信息安全管理体系是组织对其信息系统建立安全管理制度、流程等		
	2	信息安全管理体系是组织建立信息安全方针和目标，并实现这些目标的相互关联或相互作用的一组要素之和		
	3	信息安全管理体系包括信息安全管理机构、体系文件及相关资源等要素		
+	4	信息安全管理体系是组织整个管理体系的一部分，它是基于业务风险方法，来建立、实施、运行、监视、评审、保持和改进信息安全		

204 S	0.400	15:43:23	15:43:40	00:17
以下开发方法可能会引起应用受到攻击是。				
+	1	使用黑名单方式禁止用户输入可能攻击网站的数据		
	2	对输出数据使用合理的编码		
	3	前后端做好数据验证		
	4	关闭网页调试信息选项		

205 S	0.000	15:43:40	15:44:03	00:23
关于邮件安全设备描述不正确的是？				
解释 解析：				
	1	具备一定的恶意软件检测能力		
	2	具备一定的邮件系统自身漏洞防护功能		
-	3	部分设备支持旁路部署		
	4	一般都支持钓鱼网址检测		

206 S	0.400	15:44:03	15:44:08	00:05
以下哪个不是属于web应用的漏洞？				
解释 解析：2 考察web漏洞类型的了解				
	1	XSS		
+	2	buffer overflow		
	3	SQL注入		
	4	CRSF		

207 S	0.400	15:44:08	15:44:26	00:18
分布式关系型数据库与集中式的关系型数据库相比在以下哪个方面有缺点？				
	1	灵活性		
+	2	数据备份		
	3	可靠性		
	4	自主性		

208 S	0.400	15:44:26	15:44:39	00:13
dbo代表的是				
	1	用户		
	2	系统管理员		
+	3	数据库拥有者		
	4	系统分析员		

209 S	0.400	15:44:39	15:44:49	00:10
常规端口扫描和半开式扫描的区别是				
	1	没什么区别		
	2	半开式采用UDP方式扫描		
	3	扫描准确性不一样		
+	4	没有完成三次握手，缺少ACK过程		

210 S	0.400	15:44:49	15:45:51	01:02

以下哪个是 ARP 欺骗攻击可能导致的后果		
+	1	ARP 欺骗可导致目标主机无法访问网络
	2	ARP 欺骗可导致目标主机的系统崩溃，蓝屏重启
	3	ARP 欺骗可导致目标主机死机
	4	ARP 欺骗可直接获得目标主机的控制权

211 S	0.400	15:45:51	15:46:11	00:20
关于外包服务商管理，以下错误的是？				
	1	应与外包服务商建立有效的联络、沟通和信息交流机制，通过建立恰当的应急预案，以应对外包服务商在服务过程中可能出现的重大缺失或意外终止风险		
	2	重要外包项目合同签订前应对外包商开展必要的尽职调查		
+	3	应尽量将外包业务集中于单一外包商，便于对外包商的管理		
	4	应对重要外包商的财务、内控及安全管理进行持续监控，发现外包商出现异常情况时，应及时督促外包商采取纠正措施		

212 S	0.400	15:46:11	15:46:57	00:46
在安全日志管理系统进行日志实时关联分析时，以下哪一项技术措施不是提高分析准确性的基础？				
	1	设备时间同步		
	2	日志处理速度		
	3	日志字段解析		
+	4	大容量存储		

213 S	0.000	15:46:57	15:47:08	00:11
X-Frame-Options Headers设置中，哪一项配置是网站页面只能被本站页面嵌入？				
	1	DENY		
	2	ALLOW-FROM		
-	3	SAMEORIGIN		
	4	ANY		

214 S	0.400	15:47:08	15:47:26	00:18
EFS可以用在什么文件系统下				
	1	FAT32		
+	2	NTFS		
	3	FAT16		
	4	这些都可以		

215 S	0.400	15:47:26	15:47:37	00:11
以下说法正确的是				
	1	防火墙能防范新的网络安全问题		
	2	防火墙能防范数据驱动行攻击		
+	3	防火墙不能完全阻止病毒的传播		
	4	防火墙不能防止来自内部网的攻击		

216 S	0.400	15:47:37	15:47:43	00:06
在信息安全管理中采取措施可以有效解决人员安全意识薄弱问题。				
+	1	责任追查和惩处		
	2	安装终端管理系统		
	3	安全教育和培训		
	4	部署内容监控系统		

217 S	0.400	15:47:43	15:47:45	00:02
C++中this指针传参时通常存于哪个寄存器中？（架构为x86）				
	1	edx		
+	2	ecx		
	3	eax		
	4	ebx		

218 S	0.400	15:47:45	15:47:47	00:02
事务处理完成后，系统会置于处理前的状态，这个符合事务的				
+	1	一致性		
	2	持续性		
	3	原子性		
	4	隔离性		

219 S	0.400	15:47:47	15:47:51	00:04
下面的哪一种反垃圾过滤技术可以最大程度地避免正常的、长度不定的、内容里存在多处垃圾邮件关键词的电子邮件被识别为垃圾邮件？()				
	1	启发式的过滤技术		
+	2	基于统计（学）的贝叶斯判断（Bayesian）		
	3	基于签名的检查		
	4	模版匹配		

220 S	0.000	15:47:51	15:48:10	00:19
哪一项不属于邮件安全问题带来危害？				
解释 解析：				
-	1	垃圾邮件		
	2	泄露敏感数据		
	3	系统漏洞		
	4	传播勒索软件		

221 S	0.400	15:48:10	15:49:07	00:57
在部署HTTPS时，为了安全我们也会同时增加DNS CAA记录，以下哪个是DNS CAA的正确说明				
+	1	Certification Authority Authorization，证书颁发机构授权，只允许某些证书颁发机构对DNS颁发证书		
	2	Certification Authority Authentication，证书颁发机构认证，对当前的颁发机构进行认证		
	3	Complete Authentication Authorization、完全认证授权，对DNS条目进行完全的认证和授权检查		
	4	Complete Authentication Audit、完全认证审计，对DNS条目进行完全的认证和审计		

222 S	0.400	15:49:07	15:49:15	00:08
下列哪一下现象说明消息在传递过程中被修改了？				
	1	私钥密码改变		
	2	公钥密码改变		
+	3	消息摘要改变		
	4	消息被加密		

223 S	0.400	15:49:15	15:50:09	00:54
信息安全管理体系中的“管理”是指。				
	1	通过行政管理的手段，以期有效达到组织信息安全目标的活动		
+	2	通过计划、组织、领导、控制等环节来协调人力、物力、财力等资源，以期有效达到组织信息安全目标的活动		
	3	对信息、网络、软硬件等进行管理，		
	4	对组织人、财、物以及生产流程的管辖		

224 S	0.400	15:50:09	15:50:50	00:41
以下哪种是Let's Encrypt可以签发的证书：				
+	1	UCC/SAN（多域名）证书		
	2	代码签名证书		
	3	EV（扩展验证）证书		
	4	OV（组织验证）证书		

225 S	0.000	15:50:50	15:52:02	01:12
《信息安全等级保护管理办法》中，受理备案的公安机关应当对信息安全等级保护工作情况进行检查。对哪一级别的系统需要至少每半年检查一次？				
-	1	三级		
	2	二级		
	3	一级		
	4	四级		

226 S	0.000	15:52:02	15:52:05	00:03
某网站由于防火墙电源模块问题导致机柜电源出现问题，引起网站访问问题，以下哪种做法可以有效避免此问题？				
-	1	更换可靠性更高的电源模块		
	2	使用双电源		
	3	设备分布于不同的机柜		
	4	使用双路电源		

227 S	0.400	15:52:05	15:52:16	00:11
第一个实用的、迄今为止应用最广的公钥密码体制是				
	1	NTRU		

	2	Elgamal
+	3	RSA
	4	ECC

228 S	0.000	15:52:16	15:53:10	00:54
内存完整性校验不可以检查到下列哪些操作				
解释 解析：3 对内存完整性检测的了解				
	1	内存断点		
	2	内存patch		
-	3	inline hook		
	4	软断点		

229 S	0.400	15:53:10	15:54:18	01:08
2014年2月27日，中央网络安全和信息化领导小组宣告成立，在北京召开了第一次会议。中共中央总书记、国家主席、中央军委主席习近平亲自担任组长；李克强、刘云山任副组长。以下哪一项不是该小组的主要职能？				
	1	研究制定网络安全和信息化发展战略、宏观规划和重大政策		
	2	推动国家网络安全和信息化法治建设，不断增强安全保障能力		
	3	着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题		
+	4	推进安全可控关键软硬件应用，加强移动应用商店和应用程序安全管理，加强新技术新业务网络安全管理，强化网络安全技术能力和手段建设。		

230 S	0.400	15:54:18	15:54:47	00:29
下列哪项不属于操作系统自身的安全技术				
解释 解析：2 考察操作系统安全机制的了解				
	1	ASLR		
	2	CANNARY		
+	3	SEH		
	4	DEP		

231 S	0.400	15:54:47	15:54:57	00:10
以下哪个说法正确？				
解释 解析：				
	1	发件人名称是老板，所以立即执行邮件中的要求		
	2	邮件附件的后缀名是doc		
+	3	恶意邮件不一定包含附件		
	4	因为自己从来不通过邮件收发敏感数据，所以即使邮件账户被里也不会造成任何危害		

232 S	0.400	15:54:57	15:55:11	00:14
在数据管理中，对于重要的数据应该进行全生命周期的管理，除加强审计监控外，以下哪项技术也有助于对数据的生命周期进行追踪？				
解释 解析：				
	1	脱敏技术		
	2	加密技术		
+	3	水印技术		
	4	漏扫技术		

233 S	0.400	15:55:11	15:55:19	00:08
在机房或其他数据处理环境中，较高的潮湿环境会带来如下哪些弊端？				
	1	产生静电		
	2	B+A		
	3	有污染物		
+	4	计算机部件腐蚀		

234 S	0.400	15:55:19	15:55:33	00:14
下列哪个类型漏洞可用于钓鱼植入攻击？				
解释 解析：2 考察对漏洞类型的理解				
	1	永恒之蓝		
+	2	Office文件格式漏洞		

	3	SQL注入漏洞	
	4	CPU幽灵、熔断漏洞	

235 S	0.000	15:55:33	15:55:57	00:24
SSH远程登录时候，使用方式登陆管理远程SSH，禁止直接SSH密码直接登录，这样黑客拿到SSH用户密码也没用。				
-	1	ssh-rsa证书		
	2	ssh-keygen证书		
	3	ssh-key证书		
	4	ssh-login证书		

236 S	0.400	15:55:57	15:56:38	00:41
Unix系统中的last命令用来搜索来显示自从文件创建以来曾经登录过的用户，包括登录/退出时间、终端、登录主机IP地址。				
+	1	wtmp/wtmpx文件		
	2	lastlog文件		
	3	utmp/utmpx文件		
	4	attc文件		

237 S	0.000	15:56:20	15:56:46	00:26
TCP / IP协议存在漏洞可能导致的安全威胁是。				
	1	会话劫持		
	2	口令攻击		
-	3	缓冲区溢出		
	4	网络窃听		

238 S	0.400	15:56:46	15:57:01	00:15
域名服务系统（DNS）的功能是（ ）				
	1	完成主机名和IP地址之间的转换		
+	2	完成域名和IP地址之间的转换		
	3	完成域名和网卡地址之间的转换		
	4	完成域名和电子邮件地址之间的转换		

239 S	0.400	15:57:01	15:58:10	01:09
数据库的概念模型独立于				
	1	现实世界		
	2	信息世界		
	3	E-R图		
+	4	具体的机器和DBMS		

240 S	0.000	15:57:53	15:57:56	00:03
Apache Tomcat 默认配置中，除了对jsp文件的解析之外，还支持下列那种类型的文件？				
	1	.jspf		
	2	.jspx		
-	3	.action		
	4	.do		

241 S	0.400	15:57:56	15:58:00	00:04
以下哪个在邮件附件后缀中出现的扩展名最有可能是病毒？				
+	1	.ppt.exe		
	2	.doc		
	3	.com.vbs.txt		
	4	.wmv.bat		

242 S	0.400	15:58:00	15:58:16	00:16
以下哪一项面向对象的技术特征可以提高数据的安全级别？				
+	1	封装		
	2	继承		
	3	多态性		
	4	动态仓库		

243 S	0.400	15:58:16	15:58:29	00:13
下列哪个是识别是否发生系统攻击所必须的？				
	1	被动式蜜罐		

+	2	日志分析
	3	分布式防病毒系统
	4	状态检测防火墙

244 S	0.400		15:58:29	15:58:54	00:25
以下哪种特征说明一定未使用Apache Struts2框架					
	1	URL 含 .jsp			
	2	URL 含 .action			
+	3	URL 含 .php			
	4	URL 含 .do			

245 S	0.400		15:58:39	15:59:02	00:23
以下哪种漏洞通常不会导致控制流劫持？					
	1	堆溢出			
+	2	内存泄露			
	3	栈溢出			
	4	格式化字符串			

246 S	0.000		15:59:02	15:59:33	00:31
组织在建立安全管理体系过程中，首先应该建立的是以下哪一类文档？					
	1	指导方针（guideline）			
	2	策略（policy）			
-	3	规程（procedure）			
	4	标准（standard）			

247 S	0.400		15:59:33	15:59:56	00:23
ITAF深度防御战略的三个层面不包括。					
	1	人员			
	2	运行			
	3	技术			
+	4	法律			

248 S	0.000		15:59:56	16:00:24	00:28
为什么出现计算机安全事件后必须立即报告？					
	1	如果不能及时发现可能会造成更大的损失			
	2	有利于执法人员展开调查以便追查黑客			
	3	有利于用户了解这些潜在的威胁			
-	4	有利于对风险进行分析以便采取更好的防范措施			

249 S	0.400		16:00:24	16:00:38	00:14
PPTP、L2TP和L2F隧道协议属于协议。					
	1	第三层隧道			
	2	第四层隧道			
+	3	第二层隧道			
	4	第一层隧道			

250 S	0.400		16:00:38	16:01:11	00:33
_____应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助					
	1	任何人			
	2	网信部门和有关部门			
+	3	网络运营者			
	4	网络使用者			