1、小李为公司的渗透测试技术工程师，平时需要对网站进行渗透测试，他经常使用的命令有：Ping 命令、Tracert 命令、Netstat 命令，作为渗透测试工程师，小李收集了一些 exp 套件，通过一些漏洞扫描，再结合 exp 套件可以渗透到系统内部，渗透结束后小李还会将整个渗透测试过程写成报告。渗透测试报告中不会出现哪些内容?
A.漏洞的数量
B.漏洞的利用效果
C.渗透测试工程师的个人联系方式
D.用户的数据内容
答案：　BD
解析：　无

2、小李为公司的渗透测试技术工程师，平时需要对网站进行渗透测再结合 exp 套件可以渗透到系统内部，渗透结束后小李还会将整个渗透测试过程写成报告。以下关于 exp 套件的描述中，哪些选项的描述是正确的?
A.EXP，Exploit，中文意思是“漏洞利用”。意思是一段对漏洞如何利用的详试，他经常使用的命令有：Ping 命令、Tracert 命令、Netstat 命令，作细说明或者一个演示的漏洞攻击代码，可以使得读者完全了解漏洞的机为渗透测试工程师，小李收集了一些 exp 套件，通过一些漏洞扫描，理以及利用的方法。
B.EXP，Exploit，中文意思是”漏洞利用”。意思是漏洞报告中的 EXP 是一段
说明或者一个攻击的样例，使得读者能够确认这个漏洞是真实存在的。
C.先有漏洞再有 EXP 套件，它可以帮助渗透测试工程师攻破带有漏洞的系统
D.EXP 可以有效的攻击未被公布的漏洞，也称之为 O day
答案：　ABCD
解析：　无

3、小李为公司的渗透测试技术工程师，平时需要对网站进行渗透测试，他经常使用的命令有：Ping 命令、Tracert 命令、Netstat 命令，作为渗透测试工程师，小李收集了一些 exp 套件，通过一些漏洞扫描，再结合 exp 套件可以渗透到系统内部，渗透结束后小李还会将整个渗透测试过程写成报告。Ping 命令、Tracert 命令、Netstat 命令可以对哪些信息进行收集?
A.主机存活性探测
B.主机漏洞情况查看
C.当前正在工作的网络连接的详细信息看
D.数据包到达目标主机所经过的路径
答案：　ABCD
解析：　无

4、Burpsuite 能够拦截到以下哪些代码?
A、HTML 代码
B、JavaScript 代码
C、PHP 代码
D、XML 代码
答案：　ABCD
解析：　无

5、关于主机虚拟化技术的优势，以下说法正确的是哪几项?
A、备份速度慢，回复速度快
B、大幅度降低成本
C、减少维护工作
D、人力资源要求低
答案： BC
解析： 无

6、在御界的应用场景中，平台集群化部署方式有以下哪几项特性?
A.当流量大于 10G 时可使用平台集群化部署口
B.支持硬件设备按需平行扩展
C.当有多个边界点的流量需要采集，且总分析流量小于 10G 时，可采用多探针部署模式
D.使用单点部署模式时，高级威胁检测系统的分析平台、沙箱和流量探针可部署在单台服务器上
答案： ABCD
解析： 无

7．入侵检测系统使用入侵检测技术对网络和系统进行监视，并根据监视结果采取不同的处理，最大限度地降低了入侵危害的可能。以下关于入侵检测系统的叙述，描述错误的是哪项?
A.入侵检测系统可以弥补安全防御系统的漏洞和缺陷
B.入侵检测系统很难检测到未知的攻击行为
C.基于主机的入侵检测系统可以精确地判断入侵事件
D.基于网络的入侵检测系统主要用于实时监控网络关键路径的信息
答案： D
解析： 无

8.某信息系统损害后会对国家安全造成一般损失，请计算该系统的初步确认等级应该为几级?
A、2 级
B、3 级
C、4 级
D、5 级
答案： C
解析： 无

9. 对于捕获过滤器，若要表示显示来源 IP 地址为 192.168.108.128，但目的地不是 172.16.0.0/16 的封包，则以下哪一项过滤表达式是正确的?
A.dst host 192.168.108.128 or !dst net 172.16.0.0/16
B.dst host 192.168.108.128 and not dst net 172.16.0.0/16
C.src host 192.168.108.128 or !dst net 172.16.0.0/16
D.src host 192.168.108.128 and not dst net 172.16.0.0/16
答案： D
解析： 无

10.在互联网中，以下哪个是超文本传输协议的简称?
A、FTP
B、HTTPS
C、HTTP
D、TCP
答案：　C
解析：　无

11. 以下哪一个是云计算专用测试工具?
A、主机扫描工具
B、虚拟化漏洞
C、数据库扫描工具
D、流量分析工具
答案：　B
解析：　无

12. 下列哪一项使用了恶意代码的文件传播放方式?
A、垃圾邮件
B、利用系统漏洞
C、U 盘感染
D、破解软件后门
答案：　A
解析：　电子邮件是传播恶意代码的重要途径，为了防止电子邮件中的恶意代码的攻击，用纯文本方式阅读电子邮件，文本文件通常不会受电子邮件中的恶意代码的感染或携带恶意代码。

13. 关于云计算的 laaS 是一种怎样的服务类型，以下哪一个选项的描述是正确的?
A.向云计算提供商的个人或组织提供虚拟化计算资源，如虚拟机、存储、
网络和操作系统。
B.为开发人员提供通过全球互联网构建应用程序和服务的平台。Paas 为开发、测试和管理软件应用程序提供按需开发环境。
C.通过互联网提供按需软件付费应用程序，计算提供商托管和管理软件应用程序，并允许其用户连接到应用程序并通过全球互联网访问应用程序。
D.是一种基于互联网的计算方式，通过这种方式，共享的软硬件资源和信息可以按需求提供给计算机各种终端和其他设备，使用服务商提供的电脑基建作计算和资源。
答案：　D
解析：　无

14. 下列哪一项技术没有应用在 HTTPS 中?
A、SSL
B、对称加密算法
C、非对称加密
D、DHCP
答案：　D

解析： 无

15. 信息安全保障的最终目的是什么?
A、保证信息系统不被攻击
B、降低系统被攻击所售的损失
C、实现组织机构的使命
D、保证人员的安全性
答案： A
解析： 保护信息免受各种威胁的损害。以确保业务的连续性

16. 下列哪些属于网络黑产?
1、勒索病毒
2、肉鸡矿业
3、DDos 攻击
A、1、2
B、2、3
C、1、3
D、全部
答案： D

17. 小李是信息部的信息安全工程师，负责单位网站的渗透测试工作，小李今天有几个任务需要完成，如果你是小李，你会怎么解决?请小李在 Windows 10 操作系统重置密码，需要执行以下哪些操作步骤?
A. 通过加载一张刻录好 Windows 10 的光盘或者 U 盘，通过 Shift+F10 调出命令提示符，输入 regedit 调出注册表界面
B. 点击菜单栏文件-加载配置单元，找到系统盘:\Windows\System32\config\SYSTEM,选中 SYSTEM 后，点击“打开"进行加载，此时需要自拟一个临时的项名称，如"tencent" ，定位到 HKEY_LOCAL_MACHINE\tencent\Setup,在右边找到 cmdline,双击后将数值数据赋值为 cmd.exe
C. 重新开机时，会绕过密码直接登录到系统
D. 重新开机启动时，目标主机会弹出 cmd,并且权限是 system 权限，这时就可以修改密码了
答案： ABCD
解析： http://www.360doc.com/content/17/0417/19/31544578_646359055.shtml

18. 小李是信息部的信息安全工程师，负责单位网站的渗透测试工作，小李今天有几个任务需要完成，如果你是小李，你会怎么解决?在以下选项中，小李可以选择能够提升权限的方法有哪些?
A. 操作系统命令权限提升
B. 服务器软件权限提升
C. 操作系统溢出漏洞权限提升

D. 数据库存储过程/UDF 提权
答案： ABCD
解析： 无

19. 小李是信息部的信息安全工程师，负责单位网站的渗透测试工作，小李今天有几个任务需要完成，如果你是小李，你会怎么解决?请小李选出针对 IBM Rational AppScan 与 Nessus 描述最准确的两个选项?

A. IBM Rational AppScan 主要是 Web 漏洞扫描器，可以扫描如 SQL 注入(SQL-injection)、跨站点脚本攻击(cross-site scripting)及缓冲溢出(buffer overflow)、HTTP 响应拆分漏洞、参数篡改、隐式字段处理、后门/调试选项等等

B. IBM Rational AppScan 功能十分丰富，除了日常网站扫描功能外，还附带漏洞攻击，漏洞提权功能

C. Nessus 有家庭版和商业版两个版本，家庭版为免费版，商业版为付费版，他们的区别是界面不同

D. Nessus 为服务器漏洞扫描器，可以扫描服务器上的组件、微软系统、linux 系统的漏洞、多平台的应用软件漏洞

答案： AD
解析： 无

20. 某一天，公司要求信息部进行安全技能水平测试的抽查，小陈刚好被抽到，需要回答几个问题。但小陈因为没有熟练掌握相关知识和技能，一时之间，不知所措，你能帮帮小陈吗?
对于 Wireshark 的描述,正确的是以下哪几项?
A. Wireshark 不能用来做入侵检测系统

B. 对于网络上的异常流量行为，Wireshark 不会产生警示或是任何提示

C. Wireshark 只会反映出当前流通的数据包信息

D. Wireshark 本身不会提交数据包至网络上

答案： ABCD
解析：
Wireshark 不是入侵侦测软件（IntrusionDetectionSoftware,IDS）。对于网络上的异常流量行为，Wireshark 不会产生警示或是任何提示。然而，仔细分析 Wireshark 截取的数据包能够帮助用户对于网络行为有更清楚的了解。 Wireshark 不会对网络数据包产生内容的修改，它只会反映出当前流通的数据包信息。Wireshark 本身也不会提交数据包至网络上。就是说你只能查看数据包，不能修改或转发。

21. 某一天，公司要求信息部进行安全技能水平测试的抽查，小陈刚好被抽到，需要回答几个问题。但小陈因为没有熟练掌握相关知识和技能，一时之间，不知所措，你能帮帮小陈吗?
对于 Wireshark 软件中的捕捉过滤器和显示过滤器的作用，描述正确的是哪几项?
A. 捕捉过滤器用于决定将什么样的信息记录在捕捉结果中，需要在开始捕捉前设置

B. 显示过滤器在捕捉结果中进行详细查找，可以在得到捕捉结果后随意修改
C. 在捕捉过滤器的表达式中，逻辑运算符 not、or、and 拥有相同的优先级
D. 在显示过滤器的表达式中，逻辑运算符运算应从右向左进行
答案： AB
解析： not 具有最高的优先级，运算的时候优先运算 not；其次 or 和 and 具有相同的优先级，运算的时候依次从左向右计算。

22. 某一天，公司要求信息部进行安全技能水平测试的抽查，小陈刚好被抽到，需要回答几个问题。但小陈因为没有熟练掌握相关知识和技能，一时之间，不知所措,你能帮帮小陈吗?在 wireshark 捕获的信息中分析得到，公司服务器有大量的 HTTP 请求，并且大部分请求都为 POST，访问的还是 login 登录页面，则以下哪几项攻击类型是不可能出现的?

A. 提权
B. 协议欺骗
C. SQL 注入
D. 口令爆破
答案： AB
解析： 无

23. 某公司安全主管为了测试安全部门员工的安全水平，让部门员工完成以下几个问题:以下针对敏感信息泄露漏洞中，关于泄露的文件的描述， 错误的是哪几项?
A. 网站安装页: 模板网站都有一个 instal 的目录，如安装后未锁定或者未移除有可能造成网站数据库密码泄露或者网站被重置的风险
B. 网站备份文件: 网站备份文件有可能存放在 bak 目录或者直接存放在根目录，属于敏感文件
C. 网站用户: 一般网站用户具有登录会员后台的权限，这个网站用户有可能可以渗透到网站后台
D. 网站数据库: 网站数据库股都是暴露在某个文件夹中， 直接访问 db 文件夹定可以访问到网站数据库
答案： CD
解析： 无

24.某公司安全主管为了测试安全部门员工的安全水平，让部门员工完成以下几个问题:以下步骤是反射型跨站的实施过程的有哪几项?
A. 黑客以某种方式发送 xss 的 http 链接给用户

B. 用户点击链接登录网站，登录期间打开了黑客的 xss 代码

C. 网站执行 xss 攻击脚本，用户页面跳转到黑客网站，黑客获取用户信息

D. 黑客使用用户信息登录网站，完成攻击

答案： ABCD
解析：跨站脚本攻击（CrossSiteScripting）,为不和层叠样式表（CascadingStyleSheets,CSS）

的缩写混淆,故缩写为 XSS，分为反射型、存储型和 DOM 型。其攻击过程为以下步骤：1.黑客以某种方式发送 xss 的 http 链接给用户；2.用户登录网站，登陆期间打开黑客发送的 xss 链接；3.网站执行 XSS 攻击脚本；4.用户页面跳转到黑客网站，黑客获取用户信息；5.黑客使用用户信息登录网站，完成攻击。

25. 某公司安全主管为了测试安全部门员工的安全水平，让部门员工完成以下几个问题:以下的 SQL 注入的防御方法错误的是哪几项?
A. 使用 PDO 技术对数据进行预处理，PDO (PHP Data Objects)是一种在 PHP 里连接数据库的使用接口，PDO 与 mysql 曾经被建议用来取代原本 PHP 在用的 mysql 相关函数，基于数据库使用的安全性，因为后者欠缺对于 SQL 注入的防护
B. 使用 JavaScript 检验用户提交的参数是否正确，如果参数不正确，则弹出非法注入，从而防御了 SQL 注入
C. 将 mysql 数据库中的 information_schema 数据库删除，可以防止黑客通过该数据库查询信息
D. 开启数据库的日志审计功能，审计到异常行为，数据库解释器会进行阻断
答案： BCD
解析： SQL 注入的防御方法：1.利用 token 来防止 CFRF；2.检查 id 是否为数字型；3.采用 PDO，预处理过的 SQL 语句模板集；4.部署 WAF。

26. 某公司鉴于人手场地和预算原因，计划使用云计算技术部署一个门户网站服务器和数据库服务器。由于网站的特殊性，该公司需要从系统层次对门户网站服务器进行配置，而数据库服务器希望能专心于数据管理，不需要去考虑数据管理之外的问题。请根据以上信息完成下列问题。某一天,该公司的员工发现网上流传出了该公司数据库服务器中的部分保密资料，以下可能是泄露原因的是哪几项?
A. 云服务商的内部工作人员窃取了数据
B. 云租户的内部工作人员泄露的数据
C. 黑客攻击了云服务商的服务器系统，并窃取了数据
D. 黑客攻击了云租客的数据服务器，并窃取了数据
答案： ABCD
解析： 无

27. 某公司鉴于人手场地和预算原因，计划使用云计算技术部署一个门户网站服务器和数据库服务器。由于网站的特殊性，该公司需要从系统层次对门户网站服务器进行配置，而数据库服务器希望能专心于数据管理，不需要去考虑数据管理之外的问题。请根据以上信息完成下列问题。对于门户网站服务器，云服务商需要负责该云服务器的哪些安全维护?
A. 虚拟监视器
B. 硬件
C. 操作系统
D. 中间件
答案： AB
解析： 云服务器属于 IaaS 产品，云服务商对于 IaaS 的管理职责包括虚拟监视器和硬件。

28. 关于 suricata 的描述中，以下哪几项是 suricata 的运行模式?
A. single 模式

B. workers 模式
C. packet 模式
D. autofp 模式
答案： ABD
解析： Suricata 有三种运行模式，分别为 single，workers，autofp。官方推荐性能最佳的运行模式为 workers 模式。single 模式：只有一个包处理线程，一般在开发模式下使用。workers 模式：多个包处理线程，每个线程包含完整的处理逻辑。autofp 模式：有多个包捕获线程，多个包处理线程。一般适用于 nfqueue 场景，从多个 queue 中消费流量来处理。

29. 超文本传输协议是一个客户端(用户)和服务端(网站)之间____和____的标准，通常使用 TCP 协议。
A. 请求
B. 申请
C. 答复
D. 应答
答案： AD
解析： 超文本传输协议（Hypertext Transfer Protocol，HTTP）是一个简单的请求-响应协议，它通常运行在 TCP 之上。HTTP 是基于客户/服务器模式，且面向连接的。典型的 HTTP 事务处理有如下的过程，1.客户与服务器建立连接；2.客户向服务器提出请求；3.服务器接受请求，并根据请求返回相应的文件作为应答；4.客户与服务器关闭连接。

30. 列选项中，哪几个选项是 DNS 欺骗的防范措施?
A. 直接用 IP 访问重要的服务
B. 加密所有对外的数据流
C. 限制发出请求的地址
D. 限制域名服务器作出响应的地址
答案： ABCD
解析： DNS 欺骗攻击防范措施，1.直接用 IP 访问重要的服务。2.加密所有对外的数据流。3.安全设置对抗 DNS 欺骗。3.1 关闭 DNS 服务递归功能；3.2 限制域名服务器作出响应的地址；3.3 限制发出请求的地址；

31. 以下哪些选项属于常见的恶意代码?
A. 网页后门
B. 系统后门
C. 系统蓝屏
D. 内核级 ROOTKIT
答案： ABD
解析： 无

32. 以下哪几个产品属于软件即服务(SaaS)?
A. 云服务器
B. 云网盘
C. 人脸识别
D. 云数据库

答案： BC
解析： 云服务器属于 IaaS；云数据库属于 PaaS。

33．以下哪些是 burpsuite 的功能?
A. Spider
B. Intruder
C. Repeater
D. Explorer
答案： ABC
解析： 无

34. HTTPS 通信过程使用了哪些密码算法类型?
A. 对称加密算法
B. 公钥加密算法
C. 古典加密
D. 数字签名
答案： ABD
解析： 为了保护数据的安全，HTTPS 运用了诸多加密算法：1.对称加密：有流式、分组两种，加密和解密都是使用的同一个密钥。例如：DES、AES-GCM、ChaCha20-Poly1305 等。2.非对称加密：加密使用的密钥和解密使用的密钥是不相同的，分别称为：公钥、私钥，公钥和算法都是公开的，私钥是保密的。非对称加密算法性能较低，但是安全性超强，由于其加密特性，非对称加密算法能加密的数据长度也是有限的。例如：RSA、DSA、ECDSA、 DH、ECDHE 等。3. 哈希算法：将任意长度的信息转换为较短的固定长度的值，通常其长度要比信息小得多，且算法不可逆。例如：MD5、SHA-1、SHA-2、SHA-256 等。4.数字签名：签名就是在信息的后面再加上一段内容（信息经过 hash 后的值），可以证明信息没有被修改过。hash 值一般都会加密后（也就是签名）再和信息一起发送，以保证这个 hash 值不被修改。

35. 腾讯御界支持的威胁检测类型包括以下哪几项?
A. 病毒检测
B. 网络入侵检测
C. 高级威胁发现
D. 实体失陷感知
答案： BCD
解析： https://cloud.tencent.com/product/nta/details

36. Suricata 在使用前需要根据实际需求进行配置，通常情况下，suricata 的进阶配置包含以下哪几步?
A. 修改 pcap-log 的默认配置
B. 开启对局域网的攻击检测
C. 修改 default-packet-size
D. 禁用 checksum
答案： ABCD
解析： 无

37. VPN 的实现，依靠的是底层的关键技术，以下 VPN 关键技术选项中，哪几项是正确的?
A. 隧道技术
B. 安全审计技
C. 加解密技术
D. 身份认证技术
答案： ACD
解析： 实现 VPN 的关键技术主要有隧道技术、加解密技术、 密钥管理技术和身份认证技术。

38. 以下哪些是上传漏洞的防御手段?
A. 对文件名是随机生成的，并且进行了 MD5 加密
B. 禁止文件上传
C. 对文件的内容进行检查
D. 将文件上传的大小限制为 100KB 以内
答案： AC
解析： 上传漏洞防御手段，1、文件上传的目录设置为不可执行。2、检查上传文件类型。3、使用随机数改写文件名和文件路径。4、单独设置文件服务器的域名。5、使用安全设备防御。

39. 关于欺骗攻击的种类描述，以下哪几项是正确的?
A. ARP 欺骗攻击
B. DNS 欺骗
C. IP 欺骗攻击
D. Smurf 攻击
答案： ABC
解析： 欺骗攻击有种类型，包括 IP 欺骗攻击、ARP 欺骗攻击、DNS 欺骗攻击、源路由欺骗攻击。Smurf 攻击是一种病毒攻击。

40. 下列选项中，哪几项是腾讯云御界产品的优势?
A. 行为覆盖与平台监控
B. 漏洞攻击检测
C. 腾讯威胁情报集合
D. 攻击链视角与大数据分析
答案： ABCD
解析： 无

41. 下列哪几项是 P2DR 模型中的步骤?
A. Plan(计划)
B. Policy(策略)
C. Detection(检测)
D. Response(响应)
答案： BCD
解析： P2DR 模型是美国 ISS 公司提出的动态网络安全体系的代表模型，也是动态安全模

型的雏形。P2DR 模型包括四个主要部分:Policy(安全策略)、Protection(防护)、Detection(检测)和 Response(响应)。1.策略:策略是模型的核心，所有的防护、检测和响应都是依据安全策略实施的。网络安全策略一般包括总体安全策略和具体安全策略 2 个部分组成。2.防护:防护是根据系统可能出现的安全问题而采取的预防措施,这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网(VPN)技术、防火墙、安全扫描和数据备份等。3.检测:当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。检测是动态响应的依据。4.响应:系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

42. 某公司的网站使用的编辑器是 EWEBeditor 编辑器，该公司怀疑黑客通过这个组件入侵到企业内网，小张是公司的信息安全工程师，他需要通过漏洞复现的方法确认漏洞的情况，请问，以下哪些是入侵 EWEBeditor 编辑器的步骤?

A. 寻找编辑器位置

B. 确认编辑器版本

C. 确认编辑器各功能位置路径

D. 参考编辑器漏洞知识库实施攻击

答案： ABCD

解析： 无

43. 以下哪些属于云计算的服务类型?

A. IaaS

B. PaaS

C. LaaS

D. SaaS

答案： ABD

解析： 云计算的服务类型仍在不断进化,但业界普遍接受将云计算按照服务的提供方式划分为三个大类：1、IaaS(Infrastructure as a Service – 基础设施即服务)；2、PaaS(Platform as a Service – 平台即服务)；3、SaaS(Software as a Service – 软件即服务)

44. 以下针对小马、大马、功能木马的描述正确的是哪些项?

A. 都是由程序语言编写的恶意功能的程序代码

B. 它们的区别在于代码量的不同、体积大小的不同 C. 它们的区别在于代码量不同，但体积大小相同

D. 小马隐蔽性最好，但功能最少

答案： ABD

解析： 小马、大马、功能木马由于代码量不用，体积不同，因此功能各不相同。小马一般指功能较简单木马，隐蔽性非常好。但总而言之，他们都是由脚本语言编写的恶意程序。

45. 现阶段网络流量分析技术在实际环境中，得到了广泛的应用。以下对网络流量分析技术的作用，描述错误的是哪项?

A. 提供重要应用统计分析

B. 评估分支网络的成本和价值

C. 为网络出口互联链路的设置提供决策支持

D. 提供木马等恶意程序的拦截功能
答案： ABC
解析： 无

46. 分布式拒绝服务（Distributed Denial of Serice. DDoS)攻击是指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDos 攻击，从而成倍地提高拒绝服务攻击的威力。下列关于被 DDos 攻击时的现象，描述正确的是哪几项?
A. 被攻击主机上有大量等待的 TCP 连接
B. 网络中充斥着大量的无用的数据包，源地址为假
C. 受害主机无法正常和外界通信
D. 被攻击主机系统蓝屏
答案： ABCD
解析： 无

47. 利用御界进行漏洞攻击安全事件分析，操作步骤包括以下哪几项?
A. 在御界中寻找漏洞利用的安全事件
B. 基于告警详情分析恶意请求包
C. 分析 payload 请求包
D. 协议分析比对
答案： AB
解析： 无

48. 以下哪几项代码是属于“一句话木马”?
A. ?php @eval(S_POST['pass']);?
B. %evall request("pass")%
C. %@ Page Language="Jscript"%%eval(Request.Item["pass"],"unsate");%
D. &publicKey = openssl_pkey_get_public($publicKey)
答案： ABC
解析： 常用一句话木马，Asp 一句话木马：%execute(request("value"))%Php 一句话木马：?php @eval($_POST[value]);?Aspx 一句话木马：%@ Page Language="Jscript"%%eval(Request.Item["value"])%

49. 某员工访问其公司的服务器，进行了人脸识别并输入密码，验证完毕后以获得管理员角色，该角色具备修改系统配置、安装补丁、日志审计等权限。该员工为了防止恶意代码的入侵，可以在服务器上进行哪些安全加固?
A. 关闭无用端口
B. 修改加强密码策略
C. 卸载无用软件
D. 提升安全意识
答案： ABCD
解析： 无

50.以下哪个选项不是渗透测试流程里面需要实施的?

A. 信息收集
B. 漏洞利用
C. 删除网站
D. 公开漏洞
答案： BCD
解析： 渗透测试流程是 明确目标信息收集漏洞探测漏洞验证信息分析信息获取信息整理形成报告

51. 以下哪些选项是创建用户以及提升用户为 administrators 权限的命令?
A. net user 用户 123 /add
B. net use 用户 123 /add
C. net localgroup administrators 用户 /add
D. net localgroup 用户 administrators /add
答案： AC
解析： A 选项为 Windows 命令行创建账户的命令，C 选项为添加用户进 administrators 权限组。

52. 小谢所在的公司需要部署 VPN 服务，公司选择采用 IPSec 协议作为公司连接内部网 VPN 的安全协议。具体部署实施交由小谢负责，但由于概念模糊，小谢遇到了一些问题，请问，根据以上描述，下列哪几项对 IPSec VPN 的描述是正确的?
A. 在隧道模式下，信息封装隐藏了路由信息
B. 加密 IP 地址和数据以保证私有性
C. 保证数据通过网络传输时的完整性
D. 它对主机和端点进行身份鉴别
答案： ABCD
解析： 无

53. 按照功能对木马进行分类，包括以下哪些类型?
A. 破坏型
B. 键盘记录型
C. 代理型
D. 远程访问型
答案： ABCD
解析： 无

54. 某员工访问其公司的服务器，进行了人脸识别并输入密码，验证完毕后以获得管理员角色，该角色具备修改系统配置、安装补丁、日志审计等权限。该公司服务器采用了哪几种鉴别方式?
A. 实体所知
B. 实体所有
C. 实体特征
D. 实体经验
答案： ABC
解析： 身份认证作为操作系统安全的第一道防线，是保障操作系统安全的门户。目前，身

份认证主要通过下面三种基本途径之一或其组合来实现，⑴所知，个人所知道的或掌握的知识，如口令。⑵所有，个人所拥有的东西，如身份证、护照、信用卡、钥匙或证书等。⑶特征，个人所具有的生物特性，如指纹、掌纹、声纹、脸形、DNA、视网膜等等。基于口令的身份认证技术因其简单、易用并且几乎所有的操作系统都对口令认证提供了支持，得到了广泛的使用。

55．在信息收集技术中，以下关于 intitle 搜索命令的描述哪几项是错误的?
A. 搜索数字
B. 搜索英文
C. 在页面标题中搜索
D. 在页面内容中搜索
答案：　ABD
解析：　intitle 是经常用到的高级搜索指令之一。它的含义是：返回页面标题中包含有指定关键词的页面。具体的使用方法详见链接
https://jingyan.baidu.com/article/3f16e003c21c162591c103a6.html

56. 某公司安全主管为了测试安全部门员工的安全水平，让部门员工完成以下几个问题:简述一下 CSRF 漏洞被利用的流程?①用户 C 浏览并登录授信站点 A②站点 B 要求访问站点 A 并附带恶意参数③用户 C 在没有登出站点 A 的情况下，访问恶意网站 B④浏览器带着 cookie 和 B 传递的恶意参数访问站点 A⑤验证通过，浏览器生成站点 A 的 cookie
A. ①②③④⑤
B. ①③②⑤④
C. ①⑤③②④
D. ①③②④⑤
答案：　C
解析：　跨站请求伪造（crosssiterequestforgery），是一种对网站的恶意利用的攻击,XSS 利用的是站点内的信任用户，而 CSRF 则是通过伪装来自受信任用户的请求来利用受信任的网站。其过程如下：1.浏览并登录网站；2.验证通过，浏览器生成站点 A 的 cookie；3.用户 C 在没有登出站点 A 的情况下，访问恶意网站 B；4.站点 B 要求访问站点 A 并附带恶意参数；5.根据 B 在第 4 步的要求，浏览器带着第 2 步产生的 cookie 以及站点 B 传递的恶意参数访问站点 A。

57. 某公司鉴于人手场地和预算原因，计划使用云计算技术部署一个门户网站服务器和数据库服务器。由于网站的特殊性，该公司需要从系统层次对门户网站服务器进行配置，而数据库服务器希望能专心于数据管理，不需要去考虑数据管理之外的问题。请根据以上信息完成下列问题。该公司的门户网站服务器,数据库服务器应该分别选择云计算的哪种服务模式?
A. PaaS，SaaS
B. IaaS，SaaS
C. IaaS，PaaS
D. PaaS，LaaS
答案：　C
解析：　云服务器属于 IaaS 产品，云数据库产品属于 PaaS。

58．广义的信息安全的定义是什么?

A. 建立在以 IT 技术基础上的安全范畴，是信息安全应用技术，有时也被称为计算机安全或网络安全
B. 是一个跨学科领域的安全问题，根本目的是保证组织业务的可持续性运行，建立在信息系统的整个生命周期中，涉及到了人，事，物各个方面，其不仅仅是组织业务
C. 抛弃传统的 IT 技术，着力于新的信息安全技术。
D. 不需要人为的干预，全自动的信息安全技术
答案： B
解析： 信息安全的概念，狭义上指的是:建立在以 IT 技术基础.上的安全范畴，是信息安全应用技术。广义上指的是:广义的信息安全是一个跨学科领域的安全问题，根本目的是保证组织业务的可持续性运行，建立在信息系统的整个生命周期中，涉及到了人、事、物各个方面，其不仅仅这是组织业务的附加支撑,而是组织业务的命脉。

59. 以下哪一个不是主机虚拟化安全技术?
A. Hypervisor 安全机制
B. 虚拟机隔离机制
C. 虚拟机自省技术
D. 虚拟机创建技术
答案： D
解析： 主机虚拟化安全解决方案，1.虚拟化安全防御架构；2.Hypervisor 安全机制；3.虚拟机隔离机制；4.虚拟可信计算技术；5.虚拟机安全监控；6.虚拟机自省技术。

60. 某公司鉴于人手场地和预算原因，计划使用云计算技术部署一个门户网站服务器和数据库服务器。由于网站的特殊性，该公司需要从系统层次对门户网站服务器进行配置，而数据库服务器希望能专心于数据管理，不需要去考虑数据管理之外的问题。请根据以上信息完成下列问题。如果该门户网站云服务器为普通大学校园的互联网窗口，起到学校对外介绍宣传的功能，你作为安全专家需要对该网站系统进行等保定级，请问应该拟定为几级?
A. 一级
B. 二级
C. 三级
D. 四级
答案： B
解析： 根据题干描述得知，该网站属于信息发布类的学校门户网站，根据《教育行政部门及高等院校信息系统安全等级保护定级指南》中的规定，应定为二级。

61. 以下哪个是超文本传输协议的特点?
A. 无状态
B. 有状态
C. 冗余
D. 只能传输文字
答案： A
解析： 超文本传输协议，简称 HTTP 协议，其特点是，1.客户/服务器模式，一个服务器可以为分布在世界的许多客户服务。2.简单，HTTP 本身处理简单，有效地处理大量请求,HTTP 的通信速度快。3.灵活,HTTP 允许传输任意类型的数据对象,可以通过 Content-type 来指定数据类型。4.无状态，HTTP 是无状数据对象，可缺少状态记忆，运行速度高，服务

器应答速度较快。

62. 以下关于防火墙主要技术的描述中，错误的是哪一项?
A. 包过滤技术
B. 应用代理技术
C. 地址转换技术
D. 系统探测技术
答案： D
解析： 防火墙主要技术有 4 项，1.包过滤技术；2.状态检测技术；3.NAT 技术；4.代理网关技术；

63. 御界高级威助检测系统能实时感知安全威胁，分析并记录相关安全事件。以下对于御界安全事件模块描述错误的是哪一项?
A. 安全事件包含四个列表页签: 总体感知、入侵感知、威胁情报、异常文件感知
B. 安全事件的详情页包含基本信息、攻击链还原、攻击/受害者画像、失陷指标关联信息 4 个内容
C. 总体感知页为入侵感知、威胁情报、异常文件感知事件的汇总，可查看产生的所有安全事件
D. 入侵感知详情页基本信息页签包含四个模块: 基本信息、事件描述、处置建议、归并告警
答案： B
解析： 无

64. 某公司的信息系统采用了云计算的 PaaS 的服务模式，请问该公司作为云租客需要对该系统承担哪一个安全责任?
A. 应用管理
B. 硬件维护
C. 虚拟机监控
D. 操作系统管理
答案： A
解析： 无

65. 下列哪一个协议中描述了信息安全管理系统的要求?
A. ISO/IEC 27000
B. ISO/IEC 27001
C. ISO/IEC 27002
D. ISO/IEC 27003
答案： B
解析： ISO27000 原理与术语 PrinciplesandvocabularyISO27001 信息安全管理体系—要求 ISMSRequirements(以 BS7799-2 为基础)ISO27002 信息技术—安全技术—信息安全管理实践规范(ISO/IEC17799:2005)ISO27003 信息安全管理体系—实施指南 ISMSImplementationguidelines
66. 关于业务安全，下列说法中错误的是哪一项?
A. 业务安全分为广义和狭义

B. 广义的业务安全不包括硬件平台安全
C. 业务安全是指保护业务系统免受安全威胁的措施或手段
D. 狭义的业务安全指业务系统自有的软件与服务的安全
答案： B
解析： 业务安全的广义上指的是包括业务运行的软硬件平台（操作系统、数据库等）、业务自身系统（软件或设备）、业务所提供的服务的安全。

67. 下列哪一项不是常见的网络流量分析技术?
A. 基于 NetFlow 的流量分析技术
B. 基于 SMTP 的流量分析技术
C. 基于硬件探针的流量分析技术
D. 基于实时抓包分析的流量分析技术
答案： B
解析： 常用的网络流量分析方法：1.NetFlow 基于 NetFlow 的流量分析技术；2.SNMP 基于 SNMP 的流量分析技术；3.硬件探针基于硬件探针的流量分析技术；4.实时抓包基于实时抓包分析的流量分析技术。

68.
入侵检测系统(Intrusion Detetion System，IDS)是指监视入侵或者试图控制你的系统或者网络资源行为的系统，下列关于入侵检测系统功能描述错误的是哪一项?
A. 检测网络中的攻击行为，网络异常流量的检测
B. 网络数据包的拦截和过滤
C. 识别非法用户及合法用户的越权行为
D. 攻击事件或网络风险的统计分析
答案： B
解析： 入侵检测系统的作用：IDS 的作用、监控网络和系统、发现入侵企图或异常现象、实时报警、主动响应、审计跟踪。B 选项，网络数据的拦截和过滤是入侵防御系统的功能，而非入侵检测系统的功能。

69. 在信息收集技术中，allintext 搜索命令是做什么的?
A. 搜索电话列表
B. 搜索股票信息
C. 显示网页的缓存版本
D. 在网页内容里查找字
答案： D
解析：
allintext:搜索返回的是页面正文中包含多组关键词的页面。（百度不支持）。详细链接
https://cloud.tencent.com/developer/article/1562192

70. 现有捕获过滤器表达式: "src host 10.7.2.12 and not dst net 10.200.0.0/16"，下列选项对该表达式描述正确的是哪一项?
A. 显示来源 IP 地址为 10.7.2.12,同时目的地是 10.200.0.0/16 的封包
B. 显示来源 IP 地址为 10.200.0.0/16,但目的地不是 10.7.2.12 的封包
C. 显示来源 IP 地址为 10.7.2.12，但目的地不是 10.200.0.0/16 的封包

D. 显示来源 IP 地址为 10.200.0.0/16, 同时目的地是 10.7.2.12 的封包
答案： C
解析： 无

71. 下列哪项不是信息安全的基本属性?
A. 保密性
B. 易失性
C. 完整性
D. 可用性
答案： B
解析： 信息安全的五个基本属性：保密性、完整性、可用性、可控性、不可否认性。

72. 以下哪一个不是态势感知模型的级别?
A. 收集层
B. 感知层
C. 理解层
D. 预测层
答案： A
解析： 态势感知是感知大量的时间和空间中的环境要素，理解它们的意义，并预测它们在不久将来的状态。在这个定义中，我们可以提炼出态势感知的三个要素：感知、理解和预测，也就是说态势感知可以分成感知、理解和预测三个层次的信息处理，即： 感知：感知和获取环境中的重要线索或元素； 理解：整合感知到的数据和信息，分析其相关性； 预测：基于对环境信息的感知和理解，预测相关知识的未来的发展趋势。

73. 应对扫描的防御手段中，错误的是哪项?
A. 开启主机防火墙
B. 部署蜜罐系统
C. 伪装知名端口
D. 增加开放端口
答案： D
解析： 1.在防火墙(或 NAT)上采用更严格的过滤规则,阻止大部分扫描数据报文进入系统。2.主机系统除了必要的网络服务外,关闭其他所有的网络服务。例如，对于一台纯粹的 HTTP 服务器而言,只需要开放其 80 端口,其余的 FTP、Telnet 等等网络服务均可以全部关闭。有的主机甚至关闭了 ICMP 协议的网复报文，造成直接 ping 该主机时 ping 不通。 3.对于不需要为公众所周知的网络服务,采用更改默认端口的方法。例如,某 UNIX 只为某些特定的用户提供 FTP 服务,那么该 FTP 端口可以不用默认.端口 21,而选用另外一个值。这样非特定用户就无法使用该网络服务。 4.“微型蜜罐系统”的主要原理是用来伪造任意端口对其实施监听，监视系统是否有人入侵或者扫描你的计算机，使用前请先打开“config.ini”进行配置！ 因此主动开放更多端口不符合网络安全防御的原则，应尽可能的关闭全部未正在使用的端口，对正在使用的服务进行更改默认端口，避免被扫描到。

74. 利用 Wireshark 分析挖矿木马流量包时，对于具体流程的描述错误的是哪一项?
A. 将链接矿池的 IP 地址填入到 wireshark 的显示过滤器进行过滤
B. 将分析出来的数据流进行过滤，可以指定过滤追踪数据流的具体信息
C. 提取数据流中的链接，并尝试访问进行结果验证
D. 将追踪的数据流与门罗币的通信协议比对，最终可确认为挖矿木马的恶意流量
答案： C
解析： 挖矿木马流量包的实例分析操作流程:1.载入挖矿木马恶意流量文件 2.过滤显示矿池 IP3.追踪数据流的查看与分析 4.追踪数据流的数据过滤 5.协议比对

75. 下列哪个场景是信息安全的保密性速到了破坏?
A. 某企业的官方网站被黑客攻击，导致用户无法访问该企业的官方主页
B. 某政府网站被黑客攻击恶意篡改了主页内容
C. 小朱使用一台自动贩卖机购买饮料，由于贩卖机系统发生故障，小朱付了钱却没有拿到饮料
D. 某军事基地被黑客入侵，导致核潜艇制作资料被窃取
答案： D
解析： 无

76. 下列选项中哪项不是强制访问控制模型?
A. ACL
B. BLP
C. Biba
D. Chinese Wall
答案： A
解析： BLP 模型基于强制访问控制系统，以敏感度来划分资源的安全级别。Biba 访问控制模型对数据提供了分级别的完整性保证，类似于 BUP 保密模型，也使用强制访问控制系统。ChineseWall 安全策略的基础是客户访间的信息不会与目前他们可支配的信息产生神突。用户必须选择一个他可以访间的区域,必须自动拒绝来自其它与用户的所选区域的利益冲突区域的访问，同时包括了强制访问控制盒自主访问控制的属性。

77. 以下对隐藏账户的描述中错误的是哪项?
A. 隐藏账户通过命令行 net user 无法查看到
B. 隐藏账户通过命令行 net localgroup administrators 无法查看到
C. 隐藏账户在计算机管理->本地用户和组->用户中无法查看到
D. 隐藏账户在注册表中无法查看到
答案： D
解析： 无

78. 下列选项中哪项不是操作系统安全机制中的身份鉴别方式?
A. 实体所求
B. 实体所知
C. 实体所有
D. 实体特征

答案： A
解析： 身份认证作为操作系统安全的第一道防线，是保障操作系统安全的门户。目前，身份认证主要通过下面三种基本途径之一或其组合来实现，⑴所知，个人所知道的或掌握的知识，如口令。⑵所有，个人所拥有的东西，如身份证、护照、信用卡、钥匙或证书等。⑶特征，个人所具有的生物特性，如指纹、掌纹、声纹、脸形、DNA、视网膜等等。基于口令的身份 认证技术因其简单、易用并且几乎所有的操作系统都对口令认证提供了支持，得到了广泛的使用。

79.
以下哪项属于 Internet 的发展阶段?
A. NFSNet
B. ETHERNET
C. LOCALNETWORK
D. ARPANET
答案： A
解析： 无

80. 安全审计系统是保障计算机系统安全的重要手段之一，以下关于安全审计的作用，哪一项是错误的?
A. 检测对系统的入侵
B. 发现计算机的滥用情况
C. 提供系统运行的日志，从而能发现系统入侵行为和潜在的漏洞
D. 保证可信网络内部信息不外泄
答案： D
解析： 安全审计是指主体对客体进行访问和使用情况进行记录和审查，以保证安全规则被正确执行，并帮助分析安全事帮产生的原因。一个安全审计系统，主要有以下作用，1.对潜在的攻击者起到震慑或警告作用。2.对于已经发生的系统破坏行为提供有效的追纠证据。3.为系统安全管理员提供有何时何地的系统使用日志，从而帮助系统安全管理员及时发现系统入侵行为或潜在的系统漏洞。4.为系统安全管理员提供系统运行的统计日志，使系统安全管理员能够发现系统性能上的不足或需要改进的地方。网络安全审计的具体内容，1.监控网络内部的用户活动。2.侦察系统中存在的潜在威胁。3.对日常运行状况统计和分析。4.对突发案件和异常事件的事后分析。辅助侦破和取证。综上，安全审计主要是提供对信息的记录并对分析提供依据，因此 ABC 都是其作用，但不能保证可信网络内部信息不外泄。

81. 以下哪些工具属于漏洞扫描中能够应用的工具?
A. Appscan
B. kali Linux
C. 黑帽子
D. WVS
答案： A
解析： AppScan 是 Web 漏洞扫描工具。

82. 下列对于挖矿木马中的 stratum 矿池协议，理解错误的是哪一项?

A. stratum 协议是目前主流的矿机和矿池之间的 TCP 通讯协议

B. 所有类型的矿机和矿池连接的通讯协议都是基于 TCP 的 stratumt 协议

C. stratum 协议为 JSON 的数据格式

D. 通过检测 stratumt 协议可以发现挖矿行为

答案： B
解析： stratum 协议是目前最常用的矿机和矿池之间的 TCP 通讯协议，但是不是唯一的协议。

83. 以下关于 Wireshark 的描述错误的是哪一项?
A. Wireshark 是一款开源网络数据包分析工具
B. 可以利用 Wireshark 修改网络数据包
C. Wireshark 能实时检测网络通讯数据
D. Wireshark 可以捕捉多种网络接口类型的包
答案： B
解析： Wireshark 是一个网络抓包工具，不能修改网络数据包。

84. 黑客和溃客的区别?
A. 没有区别
B. 黑客技术比溃客厉害
C. 溃客技术比黑客厉害
D. 黑客研究技术，溃客搞破坏
答案： D
解析： 黑客[Hacker]们建设他们通常具有硬件和软件的高级知识，并有能力通过创新的方法剖析系统。“黑客"能使更多的网络趋于完善和安全，他们以保护网络为目的，而以不正当侵入为手段找出网络漏洞。溃客[Cracker]们破坏另一种入侵者是那些利用网络漏洞破坏网络的人。他们往往做一些重复的工作[如用暴力法破解口令]，他们也具备广泛的电脑知识，但与黑客不同的是他们以破坏为目的。

85. IBM AppScan 是什么类型的漏洞扫描工具?
A. 主机漏洞
B. 网络漏洞
C. Web 漏洞
D. 协议漏洞
答案： C
解析： 无

86. TCP/IP 协议中，网络互联层协议的主要安全问题有:拒绝服务、欺骗、窃听、伪造，那么利用软件工具 Sniffer 可以实现以下哪种攻击?
A. 欺骗攻击
B. 网络监听

C. DDoS 攻击
D. 截获 Windows 登陆密码
答案： B
解析： 本题考查软件工具 Sniffer 的用途。Sniffer，中文可以翻译为嗅探器，是一种基于被动侦听原理的网络分析方式。使用这种技术方式，可以监视网络的状态、数据流动情况以及网络上传输的信息。

87. 2018 年 7 月初，腾讯御见威胁情报中心发现陕西多家企业网站被植入 JS 挖矿木马，请问 JS 挖矿木马运用了下列哪项技术?
A. SQL 注入技术
B. XSS 技术
C. JavaScript 技术
D. CSRF 技术
答案： C
解析： 无

88. 以下选项中，符合”当 suricata 探测到 TTL 为 100 的 ICMP ping 包的时候，就会产生条包含文字: ‘Ping with TTL=100’的告警。”描述的规则是哪一项?

A. alert icmp any any -> any any (msg: "Ping with TTL=100"; \ ttl 100;)

B. alert udp any any -> any any (rev: "Ping with TTL=100"; \ttl 100;)

C. log icmp any any -> any any (msg: "Ping with TTL=100"; \ ttl 100;)

D. log udp any any -> any any (rev: "Ping with TTL=100"; \ttl 100;)

答案： A
解析： Suricata 的规则，是检测工具的灵魂，同样的产品，别人的好用，拦截率准确率高，误报率低，那就是人家规则写得好。具体规则编写规范请参考
https://cloud.tencent.com/developer/article/1652000

89. 下列选项中，不属于等级保护的实施流程的是哪一项?
A. 定级与备案
B. 安全建设
C. 等级测评
D. 风险管理
答案： D
解析： 等级保护的实施流程包含四个过程，1、定级与备案；2、安全建设；3、等级测评；4、监督检查。

90. 在信息安全保障模型中心 P2DR 相比 PDR 多出了哪一个环节?
A. Protection(防护)
B. Detection(检测)

C. Policy(安全策略)
D. Response(响应)
答案： C
解析： PDR 模型环节包括，防护 Protection、检测 Detection、响应 Response。P2DR 模型环节包括，策略 Policy、防护 Protection、检测 Detection、响应 Response。

91. 关于云安全的必要性，以下说法中正确的是哪一项?

A. 未来的杀毒软件可以有效的处理日益增多的恶意程序

B. 杀毒软件的特征库辨别法无法有效应对新型恶意代码的攻击

C. 云安全时代下，安全厂商依旧各自进行各自的安全服务，互不关联

D. 云安全技术利用本地计算机的病毒库进行病毒查杀

答案： B
解析： 未来杀毒软件将无法有效地处理日益增多的恶意程序。来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马，在这样的情况下，采用的特征库判别法显然已经过时。云安全技术应用后,识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库,而是依靠庞大的网络服务，实时进行采集、分析以及处理。整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。

92. 如果某个搭建在云计算平台上的网站被黑客从其官方主页使用 SQL 注入攻击，请问云租客和云服务商谁负有主要责任?
A. 云租客
B. 云服务商
C. 两者
D. 两者都不
答案： A
解析： 云服务提供商（CSP）安全责任，1.承担全部基础设施的安全；2.网络安全：承担网络隔离、安全服务白名单、外部 DDoS 攻击的防护；3.主机安全：承担虚拟化层的安全加固、系统镜像库、租户根访问权限；云租户（CSC）安全责任，1.承担虚拟机内应用的安全；2.网络安全：承担网络威胁检测、安全监控；3.主机安全：承担访问控制管理、补丁管理、配置加固、安全监控、日志分析。根据题干分析，此网站是由租户部署进行使用和管理。

93. 在 wireshark 的封包详细信息栏中第一行的"Frame"栏对应 OSI 参考模型的哪一层?
A. 数据链路层
B. 物理层
C. 网络层
D. 传输层
答案： B
解析： Frame 显示的是物理层数据帧的概况。

94. 若需要部署台腾讯御界 NIDS 设备，部署条件为:当有多个边界点的流量需要采集，且总分析流量小于 3G，则此时可使用下列哪项部署方式?
A. 单点部署
B. 多探针部署
C. 平台集群化部署
D. 混合部署
答案： A
解析： 当边界流量小于 3G 时，推荐使用单点部署模式，此时高级威胁检测系统的分析平台、沙箱和流量探针可部署在单台服务器上。详见链接
https://cloud.tencent.com/document/product/1010/31042#.E5.A4.9A.E6.8E.A2.E9.92.88.E9.83.A8.E7.BD.B2

95. 对于网络流量分析工具 Wreshark 的功能描述，错误的是哪一项?
A. Wireshark 不会处理网络事务，仅仅是监视网络
B. Wireshark 不会发送网络包或做其他交互性的使用
C. Wireshark 可以捕捉任何类型接口的流量
D. Wireshark 可以支持多种类型的协议进行解码
答案： C
解析： 无

96. 在现实应用中，入侵检测系统可根据不同的使用方法来分类， 若根据原始数据的来源，入侵检测系统可分为以下哪种类型?
A. 异常入侵检测和误用入侵检测
B. 基于主机的入侵检测、基于网络的入侵检测和基于应用的入侵检测
C. 集中式入侵检测、等级式入侵检测和协作式入侵检测
D. 离线检测系统和在线检测系统
答案： B
解析： 无

97. 在信息收集技术中，filetype 搜索命令是做什么的?
A. 搜索指定类型的文件
B. 在链接文本中查找文本
C. 在 URL 中查找
D. 搜索数字
答案： A
解析： filetype 搜索命令返回的是指定文件类型。详见链接
https://jingyan.baidu.com/article/73c3ce28f23d8de50343d9ac.html

98. 腾讯御界高级威胁检测系统的事件管理模块的组成，不包含以下哪项?
A. 失陷感知事件
B. 安全策略
C. IP 白名单
D. IOC 白名单

答案： A
解析： 御界产品事件管理模块有，1、安全策略；2、入侵感知事件；3、自定义威胁情报；4、IP 白名单；5、IOC 白名单。

99. 以下关于等级保护定级与备案的说法中，正确的是哪一个?
A. 等保的最终等级就是信息系统的业务信息保护等级
B. 所有的系统都需要备案
C. 四级的信息系统每年都要进行一次测评
D. 如果某个系统涉及到国家安全，那么这个系统等保至少要定为四级
答案： A
解析： 满足作为定级对象的三个基本特征的系统才可以作为定级对象，三个特征包括：1.具有唯一确定的安全责任单位；2.具有信息系统的基本要素；3.承载单一或相对独立的业务应用。因此 B 选项错误。第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。”这就是我们说的三级系统每年必须要做一次测评。因此 C 选项错误。如果某个系统涉及到国家安全，那么这个系统等保至少要定为三级，因此 D 选项错误。

100. 下列选项中，对规则动作描述错误的是哪一项?
A. alert:使用选定的报警方法产生报警信息，记录所有匹配的规则并记录与匹配规则相关的数据包
B. pass:如果匹配到规则后，suricata 会停止扫描数据包，并跳到所有规则的末尾
C. activate:报警并激活另一条 dynamic 规则
D. reject:ips 模式使用，如果匹配到之后则立即阻断数据包不会发送任何信息
答案： D
解析：drop ips 模式使用，如果匹配到之后则立即阻断数据包不会发送任何信息。

101. 以下关于 suricata 的描述，正确的是哪一项?
A. suricata 由 OISF 开发，是闭源软件
B. snort 是 suricata 的替代品
C. suricata 可以用来查杀病毒
D. suricata 是一个高性能的网络 IDS、IPS 和网络安全监控引擎
答案： D
解析：Suricata 是一款免费开源的网络威胁检测工具。主要用于实时入侵检测（IDS），嵌入式入侵防御（IPS）和网络安全监控（NSM）等。

102. WAPI 是我国自主制定的无线安全标准，它采用椭圆曲线密码算法和对称密码体制。与其他无线局域网安全体制相比，WAPI 的优越性体现在多个方面，以下关于 WAPI 的优越性体现错误的是哪项?
A. 采用预共享密钥 WPA-PSK
B. 真正实现双向鉴别
C. 使用数字证书进行身份验证
D. 采取了椭圆曲线密码算法

答案： A
解析： WAPI 具有的优势，1、双向身份鉴别；2、数字证书身份凭证；3、完善的鉴别协议。

103. 以下对黑客的称呼错误的是哪项？
A. 白帽子
B. 紫帽子
C. 黑帽子
D. 灰帽子
答案： A
解析： 白帽子：亦称白帽黑客、白帽子黑客，是指那些专门研究或者从事网络、计算机技术防御的人，他们通常受雇于各大公司，是维护世界网络、计算机安全的主要力量。很多白帽还受雇于公司，对产品进行模拟黑客攻击，以检测产品的可靠性。简而言之，白帽子是拥有网络安全技术的好人，是友军，不要开枪。

104. 下列哪些不属于区块链技术的基本特征？
A. 去中心化
B. 先进性
C. 匿名性
D. 独立性
答案： B
解析： 区块链基本特征，1.去中介化。2.开放性。3.自治性。4.信息不可篡改。5.匿名性。详见链接 https://cloud.tencent.com/developer/article/1459377

105. 在以下的规则关键字描述中，正确的是哪一项？
A. classtype: classtype 用于对规则进行分类及匹配的优先级进行指定
B. reference: 字段表示此条规则或 class 的匹配优先级
C. metadata: 字段表明这条规则相关信息所在 url
D. priority: suricata 遇到 priority 字段便会忽略这个字段的值
答案： A
解析： 无

106. 下列有关防火墙局限性的描述，错误的是哪一项？
A. 防火墙不能防范不经过防火墙的攻击
B. 防火墙不能解决来自内部网络的攻击和安全问题
C. 防火墙不能对非法的外部访问进行过滤
D. 防火墙不能防止策略配置不当或错误配置引起的安全威胁
答案： C
解析： 防火墙有十大局限性，一、防火墙不能防范不经过防火墙的攻击。没有经过防火墙的数据，防火墙无法检查。二、防火墙不能解决来自内部网络的攻击和安全问题。防火墙可以设计为既防外也防内，谁都不可信，但绝大多数单位因为不方便，不要求防火墙防内。三、防火墙不能防止策略配置不当或错误配置引起的安全威胁。防火墙是一个被动的安全策略执行设备，就像门卫一样，要根据政策规定来执行安全，而不能自作主张。四、防火墙不能防止可接触的人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存在于一个安全的地方。五、防火墙不能防止利用标准网络协议中的缺陷进行的攻击。一旦防火墙准许某些标准网络协议，防火墙不能防止利用该协议中的缺陷进行的攻击。六、防火墙不能防止利用

服务器系统漏洞所进行的攻击。黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击，防火墙不能防止。七、防火墙不能防止受病毒感染的文件的传输。防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒的软件，也没有一种软件可以查杀所有的病毒。八、防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或拷贝到内部网的主机上并被执行时，可能会发生数据驱动式的攻击。九、防火墙不能防止内部的泄密行为。防火墙内部的一个合法用户主动泄密，防火墙是无能为力的。十、防火墙不能防止本身的安全漏洞的威胁。防火墙保护别人有时却无法保护自己，目前还没有厂商绝对保证防火墙不会存在安全漏洞。因此对防火墙也必须提供某种安全保护。

107. 下面关于”一句话木马的描述中，错误的是哪项?
A. 需要经由黑客传到目标主机上后才能生效
B. 一句话木马只有 asp 版本，没有 php 版本的一句话木马
C. 一句话木马只有一句话
D. 该木马可以让黑客控制操作系统
答案： B
解析： 常用一句话木马，Asp 一句话木马：%execute(request("value"))%Php 一句话木马：?php @eval($_POST[value]);?Aspx 一句话木马：%@ Page Language="Jscript"%%eval(Request.Item["value"])%

108. 拒绝服务(Denial of Service, DoS）攻击是通过向服务器主机发送大量的服务请求，用大量的数据包“淹没”目标主机迪使目标主机疲于处理这些垃圾数据，而无法向合法用户提供正常服务的一种攻击。下列选项中，拒绝服务攻击的是哪一项?
A. 地址欺骗
B. 源路由攻击
C. SYN flood 攻击
D. 以上均不是
答案： C
解析： SYN Flood 是当前最流行的 DDoS（拒绝服务攻击）与 DDoS（Distributed Denial Of Service 分布式拒绝服务攻击）的方式之一，这是一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，使被攻击方资源耗尽（CPU 满负荷或内存不足）的攻击方式 。

109. 以下选项中，不属于网络流量分析工具的是哪一项?
A. tcpdump
B. wireshark
C. sniffer
D. nessus
答案： D
解析： tcpdump、wireshark、sniffer 均为抓包工具，nessus 是目前主流的系统漏洞扫描与分析软件。

110．腾讯御界支持的安装场景或专题分析不包括以下哪项?

A. 账号安全
B. 邮件安全

C. DNS 专题分析
D. 病毒查杀
答案： D
解析： 无

111. 以下选项中，不属于腾讯云御界特性的是哪一项?
A. 大数据持续分析
B. 深度检测
C. 失陷感知
D. 病毒查杀
答案： D
解析： 腾讯云御界产品六大特性，1.非侵入式安全；2.深度检测；3.失陷感知；4.大数据持续分析；5.全场景调查；6.安全大脑。

112. 关于 webshell,描述正确的是哪项?
A. ASP、PHP、ASPX、JSP、PERL、Python 等都有其对应的 webshell
B. 一般 webshell 有代码隐藏功能，一定不会被杀毒软件发现
C. 一句话 webshell 只有上传功能
D. 默认情况下 Windows 服务器可以运行任意类型的 webshell
答案： A
解析： 无

113. 以下对 Wireshark 功能界面描述正确的是哪一项?
A. 杂项:显示的是在封包列表中被选中项目的详细信息
B. 显示过滤器:提供处理当前显示过滤的方法
C. 封包列表:显示所有已经捕获的封包
D. 快捷按钮:提供快速访问菜单中经常用到的项目的功能
答案： B
解析： 此题选项 B 和选项 D 都是对的，腾讯云的考试题目有问题。

114．小明需要部署个无线网络，但在部署之前，要根据实际环境选择对应的网络拓扑，以下哪一项拓扑是不能选的?

A. 星型拓扑

B. 对等拓扑

C. 基本拓扑

D. 扩展拓扑

答案： A
解析： 无

115. 以下关于 VPN 的描述，错误的是哪一项?
A. VPN 能为使用者节约成本
B. VPN 能让数据安全传输
C. VPN 是虚拟的连接，非物理的连接
D. VPN 可以主动防御非法访问和入侵
答案： D
解析： VPN 连接（VPN Connections）是指在 Internet 公共网络上建立的一个安全的网络连接，通过为企业提供基于公网的加密通道，从而实现将企业数据中心（IDC）、内部办公网络与公有云的私有网络 VPC 安全的连接起来，因此 VPN 没有主动防御非法访问和入侵的功能

116. Ping 命令的作用是什么?
A. 权限提升的命令
B. 检测到对方 IP 的命令
C. 发送大量的 TCP 包的命令
D. 测试网络连接及信息包发送和接收状况的工具
答案： D
解析： 简单来说，ping 是用来探测本机与网络中另一主机之间是否可达的命令，如果两台主机之间 ping 不通，则表明这两台主机不能建立起连接。ping 是定位网络通不通的一个重要手段。

117. 小朱是某公司的信息安全测评人员，他在对个信息系统进行测平时，将业务信息安全等级定为 2 级，系统服务安全等级定为 4 级，请问该系统的初步安全保护等级为几级?
A. 2 级
B. 3 级
C. 4 级
D. 5 级
答案： C
解析： 安全等级保护等级一共分为 5 个等级，1 级、2 级、3 级、4 级、5 级，1 级保护等级最低，5 级保护等级最高，业务信息和系统服务两个等级中等级最高的等级为定级对象初步安全保护等级，因此为 4 级。

118. 若要使用 suricata 完成一次基于木马恶意流量的检测，则正确的操作步骤是以下哪个顺序?①载入规则②添加规则③编辑规则④测试规则
A. ③①②④
B. ①②③④
C. ③②①④
D. ③①②④
答案： C
解析： 无

119. 现代公钥密码学基于三大数学问题，不包括以下哪项?
A. 离散对数问题

B. 大整数因数分解问题
C. 背包问题
D. 椭圆曲线离散对数问题
答案： C
解析： 详见链接 https://blog.csdn.net/weixin_43250979/article/details/83375551

120. 关于 Web 服务器的安全配置，以下哪项描述错误?
A. 弱口令安全:网站服务器上线前应检查管理员密码强度
B. 加强服务器各文件夹目录权限
C. 修改后台管理员登录入口和管理地址
D. 网站下线，等安全时期再上线
答案： D
解析： 在护网时期，非核心阶段业务会进行下线，非必要服务器进行关机，但此方法并非根本解决业务系统及服务器安全漏洞的方法，属于治标不治本，D 选项不是安全配置。

121. Suricata 的配置文件采用了以下哪一种格式?
A. XML
B. HTML
C. YAML
D. CONF
答案： C
解析： Suricata 作为一款免费开源的安全工具，suricata.yaml 是 Suricata 默认的配置文件，以硬编码的形式写在源代码中,里面定义了几乎关于 Suricata 的所有运行内容，包括运行模式、抓包的数量和大小、签名和规则的属性和日志告警输出等等。详见链接 https://cloud.tencent.com/developer/article/1652000

122. 某员工访问其公司的服务器，进行了人脸识别并输入密码，验证完毕后以获得管理员角色，该角色具备修改系统配置、安装补丁、日志审计等权限。该公司服务器采用了哪种类型的访问控制模型?
A. 基于角色的访问控制模型
B. 自主访问控制模型
C. 强制访问控制模型
D. 基于任务的访问控制模型
答案： A
解析： 基于角色的访问控制（RBAC）是在上世纪九十年代被提出，是一种评估效果比较好的访问控制信息技术。在此种模型中，主体与客体并不是直接发生联系，而是增加了角色这一层次，先将访问操作的权限匹配给某些角色，然后在将这些特定的角色指定给相应的主体，通过这种方式主体就得到了对客体的访问权限。

123. 使用云计算技术生成虚拟主机，以下说法中正确的是哪一项?
A. 虚拟主机在逻辑和物理层面上都独立
B. 虚拟主机在逻辑上是独立的，在物理层面上一定不独立
C. 虚拟主机在逻辑上是独立的，在物理层面上可能独立
D. 虚拟主机在逻辑和物理层面上都不独立

答案： C
解析： 虚拟化是指通过虚拟化技术将一台计算机虚拟为多台逻辑计算机。

124. 下列哪个密码完全遵守强密码策略?
A. 123456
B. 1qaz2wsx
C. 7djh37dhj2
D. 7dhy3A-2d
答案： D
解析： 强密码要求含有：大写字母，小写字母，特殊字符，数字等;但不应该含有：用户名，用户姓名，常见单词等。

125. 仅显示 TCP 协议的统计信息的是以下哪条命令?
A. netstat -sp tcp
B. netstat -aop | find "tcp"
C. netstat -a
D. netstat -lntp
答案： A
解析： -s 按照每个协议来分类进行统计， -p 显示与连接有关的程序名和进程的 PID。

126，下列选项中，不属于 Suricata 特点的是哪一项?
A. 多线程
B. 不兼容 snort 规则
C. 支持 IPV6
D. 支持常见应用层协议解码
答案： B
解析： Suricata 特点：支持 nfqueue、支持 pcap 文件、支付 ipv6、支持多线程、兼容 snort 规则、支持数据包解码、支持应用层协议解码。

127. 下列选项中，哪一个是网络层协议的安全问题?
A. TCP 会话劫持
B. cookie 欺骗
C. IP 源地址欺骗
D. 跨站脚本
答案： C
解析： IP 地址欺骗的漏洞原理是 IP 源地址不可靠，攻击者使用其他计算机的 IP 地址来骗取与目的计算机的连接，获取信息或者特权。因此可以利用源路由机制（源路由的用户可以指定他所发送的数据包沿途经过的部分或者全部路由器），将自己的 ip 地址填入必经地址清单。预防：单播反向路径验证，当路由器在端口 X 接到数据包时，用该数据包的源 IP 检索路由表，如果找不到匹配，则判定为 IP 欺骗攻击，丢弃数据包。

128. OSI 七层模型从底层到最上层的顺序是什么?
A. 物理层,数据链路层,传输层,网络层,会话层,表示层和应用层
B. 物理层,数据链路层,网络层,传输层,表示层,会话层和应用层

C. 物理层,数据链路层,网络层,传输层,会话层,表示层和应用层
D. 物理层,数据链路层,传输层,网络层,表示层,会话层和应用层
答案： C
解析： 网络基础概念，解析省略。

129. Suricata 的运行模式，有一种是多个包处理线程，每个线程包含完整的处理逻辑。
A. Single 模式
B. Workers 模式
C. Autofp 模式
D. Packet 模式
答案： B
解析： Suricata 有三种运行模式，分别为 single，workers，autofp。官方推荐性能最佳的运行模式为 workers 模式。single 模式：只有一个包处理线程，一般在开发模式下使用。workers 模式：多个包处理线程，每个线程包含完整的处理逻辑。autofp 模式：有多个包捕获线程，多个包处理线程。一般适用于 nfqueue 场景，从多个 queue 中消费流量来处理。

130．OSI 安全体系结构定义了系统应当提供的五类安全服务，以下哪一项不属于这五类安全服务?
A. 访问控制服务
B. 数据可用性服务
C. 数据保密性服务
D. 鉴别服务
答案： B
解析： OSI 安全体系结构定义的五类安全服务：认证（鉴别）服务、访问控制服务、数据机密性服务、数据完整性服务、抗抵赖服务。

131，下列哪个选项不能评估密码系统安全性?
A. 理念安全性
B. 无条件安全性
C. 计算安全性
D. 可证明安全性
答案： A
解析： 无

132. arp -s 192.168.120.254 20-aa-20-32-C6-09 该条命令主要功能是?
A. arp 缓存表删除 IP 地址: 192.168.120.254 与 mac 20-aa-20-32-C6-09 的对应关系
B. 添加一条静态项，绑定 IP 地址: 192.168.120.254 对应 mac 20-aa-20-32-c6-0
C. 指定源地址为:192.168.120.254，目的 mac 为 20-aa-20-32-c6-09
D. 指定源地址为:192.168.120.254，设置访问控制，只允许 mac 地址为:20-aa-20-32-c6-09 访问
答案： B
解析： -s hostname hw_addr 手工加入 hostname 的地址映射关系

133．关于主机虚拟化技术，下列选项中不属于其安全问题的是哪一项?
A. DDos

B. 虚拟机逃逸
C. 信息窃取和篡改
D. SQL 注入
答案： D
解析： 虚拟化安全问题包括：信息窃取和篡改、侧信道攻击、DDos、虚拟机逃逸、Rootkit 攻击。