

## 阿里云云安全专业认证 ( ACP 级 ) 考试样题

## 一、 单选题

在众多的网络攻击类型中，“钓鱼网站”是最常见的攻击之一。钓鱼网站的页面看上去与真实网站界面完全一致，要求访问者提交账号和密码，以此来骗取用户银行或信用卡账号、密码等私人资料。以下有关钓鱼网站的传播手段，说法错误的是\_\_\_\_\_。

- a) 通过 QQ、旺旺等客户端聊天工具发送传播钓鱼网站链接
- b) 在搜索引擎、中小网站投放广告，吸引用户点击钓鱼网站链接
- c) 正规企业在官方网站的显著位置发布钓鱼网站链接
- d) 通过 Email、论坛、博客、SNS 网站批量发布钓鱼网站链接

2、 防 DDoS 攻击是阿里云云盾最主要的功能之一，为了帮助客户抵御不同规模的网络攻击，云盾提供了多种抗 DDoS 攻击的产品，其中“DDoS 基础防护”的开通方法是\_\_\_\_\_。

- a) 联系客户经理线下开通
- b) 自动开通
- c) 需要从管理控制台申请开通
- d) 提交工单，24 小时之内开通

3、 阿里云的云盾会检查通过公共互联网登录云服务器 ECS 的来源 IP，登录方式包括 SSH 和远程桌面，当来自某个 IP 的登录请求出现多次密码错误的情况时，会发出“ECS 遭遇密码暴力破解”的报警，当收到这个报警后，最安全的处理方法应该是\_\_\_\_\_。

- a) 通知自己业务平台的所有用户立即修改密码，并通过技术手段杜绝简单密码
  - b) 这个报警无关紧要，可以忽略
  - c) 立即更新云服务器 ECS 实例的系统用户的密码，并启用安全组防火墙，只允许特定 IP 连接 ECS 实例
  - d) 立即登录云服务器 ECS 实例，检查登录日志，如果没有异常登录成功的记录，可直接忽略
- 4、 A 公司管理员小牛近期发现公司的网站访问速度越来越慢，偶尔会出现无法打开的现象，从 web 日志中发现了数据被恶意爬取的行为，且并发访问量较大，这种情况下可以使用阿里云的\_\_\_\_\_安全产品进行防护。。
- a) 安全管家
  - b) 云安全中心
  - c) Web 应用防火墙 ( WAF )
  - d) 渗透测试

## 二、多选题

- 1、 云计算服务的安全需要云服务的提供方（如阿里云）、ISV（独立软件开发商）和用户来共同参与，任何一方的疏漏都可能产生安全风险。云计算服务的用户需要\_\_\_\_\_。（正确答案的数量：2 个）
- a) 加强组织内部的信息安全管理，避免敏感信息外泄
  - b) 定期修改业务系统密码
  - c) 保证云机房的多路供电
  - d) 维护物理基础设施的安全

- 2、 阿里云的云监控产品的“自定义监控”是提供给用户自定义监控项及报警规则的一项功能。 以下关于“自定义监控”的描述，正确的是\_\_\_\_\_。( 正确答案的数量：2 个 )
- a) 用户可以对自己关心的业务进行监控，将采集到监控数据上报至云监控，由云监控进行数据的处理，并根据结果进行报警
  - b) 只允许用户选择有限的固定模板，监控特定的服务器性能指标
  - c) 自定义的监控项的数量是有上限的，且上报监控数据的程序必须部署在阿里云的云服务器
  - d) 自定义的监控产生的数据可以永久免费保留在阿里云上
- 3、 最近网络安全事件中，勒索事件的比例不断上升，危害程度也越来越大，企业被要求其按照黑客指定的方式支付“赎金”，否则文件将有可能永远无法打开。以下\_\_\_\_\_措施可以帮助阿里云上的客户降低被勒索的风险。( 正确答案的数量：3 个 )
- a) 开启云服务器 ECS 的镜像和快照，每天进行备份，并保存 3 份以上的版本
  - b) 将不同业务应用放置在相同安全级别的服务器，其安全域一致，确保统一策略管理、统一防范
  - c) 如需远程运维，使用 IpsecVPN 或 SSL VPN 的远程解决方案
  - d) 各类云服务的帐号都采用 15 位以上的高强度密码
  - e) 远程运维云服务器 ECS 时直接用超级管理员帐号登录，方便随时验证

### 三、 判断题

- 1、 阿里云的云盾 DDoS 基础防护提供最高 5G 的默认 DDoS 防护能力，阿里云在此基础上，推出了安全信誉防护联盟计划，如果安全信誉分较高，可进一步提升 DDoS 防护能力。
- 2、 在使用阿里云 DDoS 高防 IP 以后，将会把系统的源站 IP 进行隐藏，从而防止黑客通过域名进行攻击。但是，如果黑客原来已经获取到了系统的源站 IP，还可以利用源站 IP 进行攻击，从而绕过 DDoS 高防 IP 的防护。因此，建议用户使用 DDoS 高防 IP 之前，最好修改一下源站的 IP 或者使用 SLB 将源站的 IP 进行隐藏。
- 3、 SNI ( Server Name Indication ) 是访问 HTTPS 服务时客户端与服务器进行 Host 信息交互的一个功能，用于精确定位客户端访问的具体域名。不支持 SNI ( Server Name Indication ) 的客户端访问阿里云云盾 WAF 加密过的 HTTPS 站点时会出现警告信息。