六、模拟题及解析

6.1 单选题

1. 网络钓鱼是尝试：

通过授权用户来限制对电子邮件系统的访问权限

通过使用网络入侵窃取数据

通过使用病毒来损坏电子邮件数据库

通过伪装成可信实体来获得信息

解析：网络钓鱼指通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息的一种攻击方式。最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。所以应该选 D 项。

2. 电子邮件炸弹通过以下哪一项来攻击某个特定实体：

跟踪电子邮件到目标地址

发送大量的电子邮件

触发高级别的安全警报

将所有电子邮件重定向到另一个实体

解析：电子邮件炸弹是最古老的匿名攻击之一，通过设置一台机器不断的大量的向同一地址发送电子邮件，攻击者能够耗尽接受者网络的宽带。故应该选择 B 选项。

3. honeypot 的目的是：

将黑客吸引到特定系统

使病毒与网络隔离

捕获软件错误

将通信重定向到特定 IP 地址

解析：蜜罐技术（Honeypot）是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。通过上述描述我们可以看到 A 选项是正确答案。

6.2 多选题

1. IPSec 如何保护通信？（请选择两个答案）

加密数据负载

对 IP 标头进行验证

组织未经授权的内容传输

将数据包路由到一个安全通道

安全地存储网络私钥

解析：IPSec（Internet Protocol Security）是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 IPSec 保护的计算机。IPSec 的公钥加密用于身份认证和密钥交换。公钥加密，也被称为"不对称加密法"，即加解密过程需要两把不同的密钥，一把用来产生数字签名和加密数据，另一把用来验证数字签名和对数据进行解密。Hash 信息验证码 HMAC（Hash message authentication codes）验证接收消息和发送消息的完全一致性（完整性）。综上所述，应该选择 A、B 两项。

2. 通过启用以下哪两项 Cookies 可以影响安全性：（请选择两个答案）

安全套接字层（SSL）

网站跟踪浏览习惯

存储网站密码

更高的安全网站保护

解析：Cookie 的目的是为用户带来方便，为网站带来增值，一般情况下不会造成严重的安全威胁。Cookie 文件不能作为代码执行，也不会传送病毒，它为用户所专有并只能由创建它的服务器来读取。另外，浏览器一般只允许存放 300 个 Cookie，每个站点最多存放 20 个 Cookie，每个 Cookie 的大小限制为 4KB。但是 Cookie 记录了用户的帐户 ID、密码之类的信息，如果被人截获并向服务器提交并且通过验证，就可以冒充受害人的身份登陆网站。所以，应该选择 B、C。