中南大学考试试卷

时间 100 分钟

网络安全 课程 48 学时 3 学分 考试形式： 开 卷

专业年级： 班 总分 100 分， 姓名

注：此页不作答题纸，请将答案写在答题纸上

一、填空题（每空 1 分，共 22 分）

（1） IPSEC 的工作模式包括模式和 模式。前者主要负责 之间的通信，后者负责 之间的通信。

（2）CA 的作用是 ，不同 CA 之间跨域信任关系可以采用信任关系和信任关系。

（3）系统的最易渗透原则是指 。

（4）列举三种恶意代码的传播方式、 和。

（5）局域网在 ARP 欺骗发生时，可能的后果包括、 等。

（6）列举几种攻击前期采用的手段、 和 。

（7）入侵检测常用的检测数据源可以是、 和 等。检测方法的基本类型可以是和 。两种类型中， 只能针对已知攻击进行检测。

二、对错题（每空 2 分，共 20 分）

（1）TLS 策略仅仅采用了对称秘钥机制。

（2）SPF 通过验证邮件的 IP 地址是否属于邮件服务器域名来识别垃圾邮件。

（3）Syncookies 机制可以抵抗大规模 SYN 攻击。

（4）防御 CSRF 攻击地方法是利用会话管理中的 cookie 认证机制。

（5）无状态防火墙可以拦截对内部 SMTP 服务器的请求，同时允许访问外部邮件服务器的请求通过。

（6）当攻击者试图进行 TCP 会话劫持时，总是会设法获取其 TCP 序列号。

（7）公钥加密算法的加密强度要由于对称密钥算法。

（8）Smurf 攻击是一种放大式拒绝服务攻击

（9）第三方可以用 CA 的私钥进行证书认证

（10）APT 攻击是一种针对具体目标的持续性的攻击。

三、（6 分）挑战应答协议通常应用于远程身份认证，相比于其他方式认证，挑战应答协议具有什么优势?

四、（6 分）假设企业防火墙的规则是五元组的规则，企业内部有一个 Web 服务器和一个邮件服务器都要开放服务，IP 地址分别是 202.197.5.1 和 202.197.5.2，请书写防火墙设置规则，允许外部的访问，同时企业有一个 FTP 服务器（IP 地址是 201.97.5.3），只允许内部网

络主机进行访问（内网段为 202.197.4.0/24），请给出在防火墙设置的通过或拦截规则。 设防火墙规则的形式为 （源地址，源端口，目的地址，目的端口，接受/拒绝）

五、（6 分）一个小型网站希望抵抗 SYN 攻击，可以通过租用大型第三方代理转接 TCP 连接服务来完成，说明其工作原理。

六、（10 分）网站的注入式漏洞产生的根本原因是什么？为什么说过滤不能算是一个好的解决方案？比较彻底的解决方案应该是什么？

七、（10 分）Gmail 采用了 DKIM 机制，当 mail.csu.edu.cn 收到一封声称来自于 Gmail 的邮件，会执行什么操作？这种机制是否可以防止网络攻击者冒充 Gmail 邮箱发送邮件，说明可以或者不可以的理由。

八、（10 分）（1）假设一个机构想阻止员工发送带有特定内容的 HTTP 请求到外部的 Web 服务器，请设计一套方案来完成这个目标。

（2）如果这是个 HTTPS 的请求,该如何来达到这个目标。

九、（10 分）请举两个例子说明当前应用的复杂性带来了更多的不安全因素和新的攻击面（例如移动应用、云计算、物联网）。