2019~2020 第二学期《计算机网络安全》考试试卷

（A 卷）开卷 考试时间：2020 年 5 月 12 日

1. **判断改错题**（判断失误不得分，错误命题判断对但未改正的小题得 1 分，共 **10 分**）

（1）采用异常检测技术的 IDS 具有误报率低，漏报率高的特点。

（2）当服务器遭受到 DoS 攻击导致不能正常提供服务的时候，重启动系统就可以解决该问题。

（3）在常规 VPN 实现中，为保证较快的运算速度和较少的运算量，在通信流量加密和密钥管理分发上通常采用对称加密算法。

（4）由于 UDP 是无连接协议，所以状态检测防火墙不对 UDP 进行状态跟踪。

（5）Syn-flood 攻击，是针对 TCP 连接的序列号生成变化的规律性进行攻击的。

2. 简述包过滤防火墙和状态检测型防火墙在处理 FTP 协议数据时的差别。**（8 分）**

3. 在 TCP SYN-flooding 攻击中，

（1）攻击者如何避免目标主机返回的报文会攻击到自己？ **（4 分）**

（2）假如在攻击机和目标主机之间加了一道防火墙，那么针对（1）中攻击者可能采取的手段，防火墙可以采取什么措施来检测到攻击，并加以防范？ **（8 分）**

4. 在用交换机连接的局域网中，能否监听到同一局域网中其他主机访问 Internet 的报文？若能，请说明理由。若不能，请说明如何才能监听到，并简述其原理。**（10 分）**

5. 假设有下列 tcpdump 的报文截获结果，判断发生了什么攻击，描述该攻击的原理和防治的方法。 **（10 分）**

```
23:29:18.503558 211.69.1.2.5133 > 211.69.1.1.139: udp 22 (frag 1021:16@0+)
23:29:18.504693 211.69.1.2 > 211.69.1.1: (frag 1021:34@16)
```

6. 某主机通过域名访问某银行网站，最后发现是个假网站，通过 DNS 解析出来的 IP 地址是错误的，有可能遭受了哪种攻击？请大致说明一下该攻击的原理。**（10 分）**

7. 如图 1 的网络环境中，主机 HA 通过路由器 RA 和 RB 到达主机 HB，主机 HA 要与主机 HB 通过 IPSec VPN 进行安全通信，安全需求如图 1 所示。

（1）考虑传输模式和隧道模式，主机 HA 应该如何封装发出的报文？写出合适的报文封装形式（假设无 NAT）。**（8 分）**

（2）IPSec 中 AH 只能实现验证功能，而 ESP 既可以实现验证，又可以实现加密。简述为什么不能用 ESP 完全取代 AH？ **（6 分）**

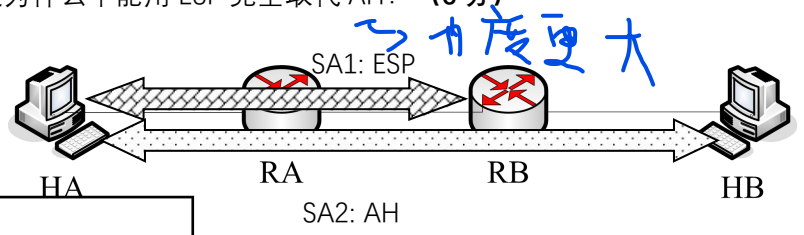

图 1

8. 一个组织的网络拓扑如图 2 所示，安全需求如下：

（1）总部的 web 服务器对 Internet 开放，但 FTP 服务器仅对本组织成员开放（包括总部、分之机构、办事处、移动用户 AB）；

（2）希望组织成员之间通信受到安全保护；

（3）总部、分支结构、办事处的网络受到安全监控和保护。

请结合你所学到的网络安全技术，在答题卡上在图中数字编号所标注的位置部署相应的安全技术产品，并简单说明其所使用的安全策略。**（16 分）**

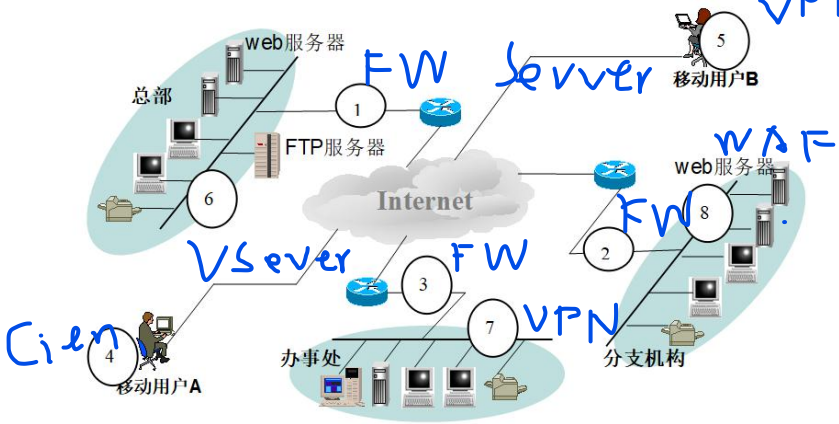

图 2

9. 针对目前你所接触到的网络系统，谈谈其中存在的安全问题，并说明你已经采取或计划采取的安全措施。（10 分）