北京邮电大学2019——2020学年第二学… 用时:01:59:20

展开 »

19 /19题

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

1.主观题 (20分)

填空题（20分，每题2分，答题时一定要写好“序号”和对应的“答案”）

1、 网络信息安全服务主要包括：_____、_____、完整性和可审性服务。

2、 访问控制策略主要包括最小特权原则、最小泄漏原则、_____。

3、 L2F工作在网络的_____层。

4、 防火墙访问控制方法主要包括：_____、方向控制、用户控制和_____。

5、 NAT技术的两个主要目的是：_____、和_____

_____。

6、 根据体系结构分类，入侵检测技术可以分为_____ 、_____和协作式。

7、 CIDF根据IDS系统的通用需求及现有IDS的系统结构，将IDS系统构成划分为四个部分，包括：_____、_____、响应单元、事件数据库。

8、 SSL协议分为两层，其中底层协议是：_____。

9、 PGP为_____和文件存储提供了认证和保密性服务。

10、 DNS查询主要包括_____和_____两种查询方式。

我的答案

1、保密性、可用性
2、多级安全策略
3、数据链路层
4、服务控制、行为控制
5、解决IP地址空间不足的问题、向外界隐藏内部网结构
6、集中式、等级式
7、事件产生器、时间分析器
8、SSL记录协议
9、电子邮件
10、递归查询、迭代查询

2.单选题 (2分)

下面的拒绝服务攻击发送的数据包是TCP协议的是（ ）。

A SYN Flood攻击

B Smurf攻击

C ICMP洪水攻击

D Ping of Death

3.单选题 (2分)

Snort属于以下哪种类型的软件（ ）。

A 远程扫描工具

B 防火墙软件

C 入侵检测软件

D 通信加密软件

4.单选题 (2分)

从实现技术分类，防火墙不包括下列选项中的哪个？（ ）

北京邮电大学2019——2020学年第二学… 用时:01:59:20

展开 »

19 /19题

B 包过滤防火墙

C 应用网关防火墙

D 电路级网关

5.单选题 (2分)

IKE协议使用（ ）算法进行密钥交换。

A ECC

B 3DES

C Diffie-Hellman

D SHA

6.单选题 (2分)

在网络通信中，下面（ ）协议能够实现链路层通信的安全性。

A SSL

B PPTP

C PGP

D IPSec

7.单选题 (2分)

IKE用于IPSec VPN建立SA时，阶段一主模式分（ ）个步骤。

A 1

B 2

C 3

D 4

8.单选题 (2分)

下面哪个不是VPN的功能（ ）。

A 数据可控性保护

B 数据完整性保护

C 数据源身份认证

D 重放攻击保护

9.单选题 (2分)

下面不属于入侵检测Denning模型中的是（ ）。

A 误用记录

B 活动档案

D 审计记录

10.单选题 (2分)

下面哪个攻击不属于拒绝服务攻击（ ）。

A SYN Flood

B Smurf攻击

C ARP欺骗

D land攻击

11.单选题 (2分)

下列关于应用网关的优点，描述错误的是（ ）

A 可以监控和过滤应用层信息

B 可以为用户提供透明的加密机制

C 允许内外网主机的直接连接

D 可以提供比包过滤防火墙更详细的日志记录

12.主观题 (6分)

DNS欺骗是攻击者常用的手段，请描述DNS欺骗的原理，并详细介绍DNS欺骗过程的各个步骤。

我的答案

答：1、DNS欺骗的原理：①DNS报文只使用序列号来进行有效性鉴别，序列号来匹配引入了序列号攻击的威胁②从协议的定义来看，在DNS应答报文中可以附加信息，该信息可以和请求的信息没有关系。这样攻击者可以随意添加信息，对网络的完整性构成威胁；③DNS的缓存机制使得主机再次查询时不需重新查询，这也会导致DNS欺骗；
2、DNS欺骗过程
（1）攻击者首先监听客户端与服务器端之间的通信
（2）客户端向服务器发送请求
（3）攻击者早于服务器向客户端发送一个假的应答包。
（4）服务器晚于攻击者发送真正的应答，但是被客户端丢弃。
（5）这样就完成了DNS欺骗的过程

13.主观题 (6分)

屏蔽子网体系结构防火墙有哪几个部分构成？详细描述各个组成部分的功能。

我的答案

答：
1、屏蔽子网体系结构防火墙由周边网络、内部网络、堡垒主机、外部路由器、内部路由器等组成。
2、各个组成部分的功能如下：
（1）周边网络：是一个防护层，放置一些信息服务器作为牺牲主机，用于承受可能受到的攻击，即使受到侵害，也会消除对内部网的侦听；
（2）内部网络：真正的信息服务器，用于存放机密信息，数据交换保存通信等；
（3）堡垒主机：位于周边网络，是整个防御体系的核心，可以运行各种代理服务程序，控制入站服务的通行；
（4）外部路由器：过滤外部网络的数据包，保护周边网络和内部网络不受外部的攻击；
（5）内部路由器：过滤外部和周边网络的数据包，保护内部网络不受外部和周边网络的攻击。

14.主观题 (6分)

Teardrop是什么类型的攻击？详细描述其攻击的原理。

1、Teardrop是典型的DoS攻击
2、Teardrop攻击的原理如下：
由于数据包传送的时候限制了数据包的大小，如果数据包过大，需要进行分段，Teardrop攻击就是利用分割重组间的漏洞，就是向目标机器发送损坏的IP包，例如重叠的或者较大的包载荷，使得接受数据方重组数据包的时候，出现数据包长度超大，甚至为负值，导致溢出的攻击。

15.主观题 (6分)

简述IPSec VPN中AH协议的功能。使用AH协议时有哪两种模式？分析这两种模式的差异。

我的答案

答：
1、AH协议的功能为：进行身份认证、数据完整性的校验以及重放攻击保护
2、使用AH协议的两种模式：
（1）传输模式，（2）隧道模式
3、这两种模式的差异：
（1）传输模式是在原始IP的头部和负载之间加入AH的头部，加密设备等同于通信设备；
（2）隧道模式是在原始IP包的前面加上AH头部，再在AH头部前加上新的IP头，加密设备不等同于通信设备。

16.主观题 (6分)

SSL有哪些主要协议？请详细描述SSL数据封装的过程。

我的答案

答：
1、SSL的主要协议有：
（1）底层的为：SSL记录协议
（2）上层的有：SSL握手协议、SSL密码变化协议、SSL警告协议
2、SSL数据封装的过程：
（1）分块：上层消息分成大小相等的小块（一般为214字节）
（2）压缩：无损压缩
（3）计算MAC：计算消息认证码
（4）加密：采用CBC模式采用指定的加密算法加密。

17.主观题 (6分)

snort使用的是哪种检测技术？这种检测技术的原理是什么？有什么优缺点？

我的答案

答：
1、snort使用的是误用检测技术
2、误用检测技术的原理为：首先通过对入侵行为的特征、环境、次序等进行描述，通过某种方式预先定义入侵行为，然后对系统进行监视，从中找出符合预先定义规则的入侵行为。
3、误用检测技术的优点：
（1）算法简单；（2）系统开销小；（3）效率高；（4）准确度高
4、误用检测技术的缺点：
（1）只能检测到已知的攻击，对于新类型的攻击无能为力；
（2）模式库要不断进行更新，知识依赖于硬件平台、操作系统和应用程序等，所以模式库的建立和维护比较难。

18.主观题 (6分)

详细列出PGP邮件加密功能的处理过程（不包括钥匙环），并简单描述处理顺序及原因。

我的答案

答：
1、PGP邮件加密功能的处理过程如下：
（1）发送方生成消息报文m1并生成随机数作为会话密钥k
（2）发送方用会话密钥加密上面的消息m1为m2
（3）发送方获取接收方的公钥，并用公钥加密会话密钥，再与加密后的消息m2结合
（4）接收方收到加密后的消息m1+m2

3、按这种顺序处理的原因是：
（1）先签名再压缩，这是因为压缩不需要为检验签名而保留压缩版本的信息；压缩算法的不同可能会导致不同的结果，这也是为了保证签名和内容的一致性；
（2）压缩之后再加密的原因是压缩后的消息冗余度更小，使得分析密码的难度更高，如果先加密再压缩，那么不能体现压缩增加冗余度的作用。

19.主观题 (18分)

移动互联网已经成为当前人们应用最广泛的网络形态之一，移动互联网的安全问题也是大家关注的重点，大量的相关安全案件也说明其是攻击的重要目标，请尝试分析下述问题并给出答案：

1、 请列举当前移动互联网存在的主要安全问题（不少于3种）；
2、 请列举你了解的移动互联网的安全措施和技术（不少于3种）；
3、 说出你针对当前问题的解决方案。

我的答案

答：
1、当前移动互联网存在的主要安全问题：
（1）个人隐私泄露；（2）钓鱼网站；（3）骚扰电话、短信、垃圾邮件；（4）互联网病毒的传播；（5）集成度高的移动智能终端设备受攻击后难以恢复等等。
2、移动互联网的安全措施和技术：
（1）国家实施网络安全法，普及网络安全知识，净化网络环境；
（2）杀毒软件对恶意软件的检测、垃圾邮件过滤功能、骚扰电话短信过滤功能；
（3）移动互联网文件访问控制，应用隐私权限白名单；
（4）移动签名服务、移动身份认证技术等等；
3、针对当前移动互联网的问题的一些看法及解决方案：
（1）首先从大的方面讲，国家和相关网络公司要投资建立专业的、系统的、相对安全的移动互联网体系，净化网络环境，提高网民的安全度；
（2）落实到个人，目前大多数的病毒传播以及网络攻击是由于个人网络安全意识匮乏，所以鼓励网民了解网络诈骗攻击的手段、提高网络保护意识、做好个人安全防护，可以很大程度解决当前移动互联网的安全问题；
（3）对于移动互联网，主要要解决移动设备的安全，比如设置好移动设备密码、传输加密、敏感操作进行身份认证、软件系统及时更新、启用白名单、支持远程禁用设备等等。