第1章 网络安全

1.网络安全的基本属性

**机密性（Confidentiality）、完整性（Integrity）、可用性（Availability），简称CIA**

2.主动攻击、被动攻击的概念、区别，哪些攻击行为是主动攻击、哪些是被动攻击

**主动攻击是指对信息流进行篡改和伪造。主要分为四类：伪装、重放、消息篡改、拒绝服务**

**被动攻击指攻击者在未授权的情况下，非法获取信息或数据文件，但不对数据信息做任何修改。常用的攻击手段有两种：消息泄露、流量分析**

**主动攻击可以检测，但难以防范；被动攻击非常难以检测，但可以防范。**

3.哪些攻击发生在TCP/IP协议簇的数据链路层、网络层、传输层（结合12章）

**数据链路层：ARP欺骗、网络嗅探**

**网络层：IP欺骗、源地址欺骗、IP分片攻击、ping和traceroute、扫描**

**传输层：利用三次握手、UDP欺骗**

4.TCP/IP协议簇的相关安全协议有什么？都发生在那一层？（结合12章）。

**数据链路层：802.1X、EAP等**

**IP层：IPSec等**

**传输层：SSL/TLS等**

**应用层：PGP，PKI、SET、SSH等**

5.OSI安全体系结构关注了哪三方面的内容？

**安全攻击、安全机制、安全服务**

第2章 网络安全威胁

6.常见的网络隐身技术包括哪些？

**IP地址欺骗、MAC地址欺骗、代理（Proxy）隐藏、网络地址转换（NAT）、账号盗用和僵尸主机等。**

7.什么是IP地址欺骗？防范IP地址欺骗的措施有哪些？

**利用主机间的正常信任关系，通过修改IP报文中的源地址，以绕开主机或网络访问控制，隐藏攻击者的攻击行为。**

**防范措施有：**

**1.在路由器上对包的IP地址进行过滤；**

**2.使用随机化的ISN，使攻击者无法猜测出正常连接的序列号；**

**3.使用加密的协议（如：IPSec、SSH等），并通过口令或证书等手段进行必要的身份认证；**

**4.不使用任何基于IP地址的信任机制。**

8.什么是MAC地址欺骗？

**攻击者将自己的MAC地址伪装成合法主机的MAC地址，诱使交换机将本应传输给合法主机的流量转发给攻击者。**

9.什么是WHOIS？

**Whois是一个Internet协议，可用于查询某个IP或域名是否注册（注册时的详细信息）、IP或域名的归属者（包括联系方式、注册和到期时间等）。Whois可以有两种：DNS Whois和IP Whois。**

10.什么是主动信息收集？什么是被动信息收集？区别是什么？

**主动信息收集是指可以通过扫描目标系统来确定目标主机开放的服务。**

**被动信息收集是指在不直接接触目标系统的情况下，获取目标主机的信息。**

**主动信息收集需要与目标主机发生接触，被动信息收集不需要。**

11.端口扫描的原理是什么？

**当一个主机向远端一个服务器的某一个端口提出建立一个连接的请求，如果对方开启此项服务，就会应答，如果对方未开启此项服务，就不会应答。**

12.端口扫描的分类有哪些？重点看：Connect扫描、SYN扫描、ACK扫描。

**TCP SYN扫描、TCP connect扫描、TCP FIN扫描、TCP ACK扫描、TCP Null扫描、TCP Xmas扫描、SYN | ACK扫描、UDP扫描、其他扫描**

13.操作系统探测的原理是什么？

**虽然TCP协议有RFC标准，但是各个操作系统实现协议栈的细节并不相同，有的实现了一些可选项，有的对TCP/IP协议进行了一定的改动。这样，有针对的对这些各个操作系统的特征发送一系列探测报文，并根据各个操作系统对探测报文的独特响应，就可以判断出目标所使用的操作系统是什么。**

14.什么是嗅探？它属于哪种攻击方式？

**嗅探是指利用计算机的网络接口截获其它计算机的数据报文的一种手段，嗅探属于被动攻击方式。**

15.什么是社会工程攻击？

**通过操纵人来实施某种行为、通过人的泄露来获取机密信息的一种攻击方式。**

16.什么是Dos？什么是DDos？

**广义而言，凡是利用网络安全防护措施不足导致用户不能继续使用正常服务的攻击手段，都称之为DoS（拒绝服务攻击）。**

**DDoS（分布式拒绝服务)攻击：指借助于C/S技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。**

17.从攻击方式上分，DoS的分类有哪些？从网络分层上分，DoS的分类有哪些？

**DoS攻击，从攻击方式上来分，可以分为两类：带宽消耗型，资源消耗型；从网络分层上来说，也可以分为两类：网络层攻击、应用层攻击。**

18.什么是缓冲区溢出攻击？

**利用程序的缺陷（没有验证缓冲区长度、程序拼接等），通过向程序提交过长的、经过精心设计的输入数据，破坏或改写内存中的关键数据，来绕过程序验证、执行恶意代码的行为。**

19.从Web访问的角度看，Web攻击有哪三个（结合12章）？

**服务器安全、客户端脚本安全、Web信道安全**

20.什么是SQL注入？它攻击的是什么？

**所谓SQL注入，就是通过把SQL命令插入到Web**[**表单**](https://baike.baidu.com/item/%E8%A1%A8%E5%8D%95/5380322)**提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。Web服务器**

21.什么是XSS？它攻击的是什么？

**通常指攻击者通过“HTML注入”篡改网页，插入了恶意的脚本，从而在用户点击链接或浏览网页时，控制用户浏览器的一种攻击。Web浏览器**

第3章 密码学概述

22.明文、密文、加密、解密的英文单词。

**明文（Plaintext）、密文（Cipher）、加密（Encryption）、解密（Decryption）**

23.密码学能做什么？靠什么实现？

**保证信息通信双方能看懂，别人看不懂。保证信息在传输过程中不被篡改（篡改可发现）。确保数据的正确来源，保证通信实体的真实性。确保通信双方对自己发送的信息不能抵赖。算法，协议。**

24.密码分析学的攻击方式有哪些？

**穷举攻击、统计分析攻击、解密变换攻击**

25.从密码攻击者所知道的资源多少来分，密码攻击分为哪些？

**唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、选择文本攻击**

26.什么是密码学上的计算上安全？它需要满足的哪两条准则？

**使用有效资源对一个密码系统进行分析而未能破译，则该密码是强的或计算上安全的。**

**1.破译密文的代价超过被加密信息的价值。**

**2.破译密文所花的时间超过信息的有用期。**

27.置换密码的单词、代替密码的单词。什么是置换密码？什么是代替密码？

**置换（Permutation）密码：对明文字符进行位置移动的密码。**

**代替（Substitute，代换）密码：将明文字符按照对应关系代替成另外的密文字符。**

第4章 对称加密

28.什么是对称加密？

**采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密。**

29.什么是流密码？

**将明文逐字符或逐位与由密钥产生的等长密钥流进行运算，产生密文。**

30.什么是分组密码？

**将明文划分为长度为m的若干个分组，各分组在密钥的控制下，变换成长度为n的密文分组。一般情况下，m=n，长度一般是64比特的倍数。**

31.在香农对于密码学的描述中，混淆（confusion）和扩散（diffusion）对加密起什么作用？

**混淆（Confusion）：尽可能的使密文和密钥之间的关系变得复杂，以阻止攻击者发现密钥。**

**扩散（Diffusion）：让每个明文数字尽可能的影响多个密文数字，使明文的统计特性消散在密文中**

32.DES算法采用了什么结构？需要多少轮迭代？密钥长度是多少？

**DES采用了Feistel结构，循环轮数为16轮，密钥长度为56比特**

33.AES算法的密钥长度有哪些？

**128/192/256比特**

34.信息安全对随机数有哪些需求？伪随机数能满足哪些？

**随机性：随机数应该不存在统计学偏差，是完全杂乱的数列。**

**不可预测性：不能从过去的序列推测出下一个出现的数。**

**不可重现性：除非数列保存下来，否则不能重现相同的数列。**

**随机性、不可预测性**

35.什么是分组密码的工作模式？了解ECB模式和CBC模式。

**工作模式是一项增强密码算法或者使算法适应具体应用的技术，NIST定义了5种工作模式：电子密码本（ECB）、密码分组链接（CBC）、密码反馈（CFB）、输出反馈（OFB）、计数器（CTR）**

第5章 公钥加密

36.什么是公钥加密（非对称加密）？

**非对称加密在加密的过程中使用一对密钥，而不像对称加密只使用一个单独的密钥。一对密钥中一个用于加密，另一个用来解密。**

37.公钥密码和对称密码的区别

**对称密码主要用于数据加/解密，公钥密码主要用于身份认证、密钥管理、数字签名等。对称密码速度快，公钥密码计算量大、速度慢。**

38.RSA算法的加密、解密过程

**私钥{e, n}，公钥{d, n}**

**私钥{5, 119}，公钥{77, 119}**

**加密：c = me mod n**

**m=19， c = 195 mod 119 = 66**

**解密：m = cd mod n**

**m = 6677 mod 119 = 19**

第6章 消息认证和散列函数

39.实现消息认证的三种方式是什么？

**消息加密、MAC、散列函数**

40.什么是Hash函数？Hash函数在密码学上的应用有哪些？

**散列函数（Hash函数、杂凑函数、摘要函数等）H：作用于任意长度的消息M，返回一个固定长度的散列值h。h = H(M)。**

**检测软件的完整性、口令保护、构造HMAC、数字签名、伪随机数生成器**

41.在密码学中对Hash函数的基本要求有哪些？

**Hash函数表示为：h=H(M)，则：**

**1.M的大小可变、h的大小固定**

**2.H函数往往是公开的，如：SHA-1、MD5等**

**3.快速，H(M)比较容易实现，用软硬件均可**

**4.单向性：知道H和h，无法反推出M**

**5.抗碰撞性：不同的数据经过哈希计算一定产生不同的哈希值，并且附带雪崩效应**

42.什么是Hash碰撞？

**简单地说，所谓哈希（hash），就是将不同的输入映射成独一无二的、固定长度的值（哈希值、摘要、指纹）。它是最常见的软件运算之一。如果不同的输入得到了同一个哈希值，就发生了哈希碰撞。**

43.什么是生日攻击？

**利用哈希空间不足够大，而制造碰撞的攻击方法，就被称为生日攻击。**

44.在密码存储中，我们常常使用的加盐指什么？

**将一个随机生成的字符串与原始密码连接在一起，然后将连接后的字符串加密。**

45.消息认证码MAC指什么？其中哪些技术保证了消息未被篡改？哪些技术保证了消息源的真实性？

**一种消息认证技术，利用带密钥的Hash函数生成一个固定大小的数据块，并将该数据块附加在消息之后。**

**Hash。密钥。**

46.构造消息认证码MAC的方法有哪些？

**使用对称加密函数、使用Hash函数构造**

47.什么是数字签名？数字签名的作用是什么？

**一种使用公钥加密技术实现的（私钥加密公钥解），用于鉴别数字信息和签名者身份的技术。类似于写在纸上的传统的物理签名。**

**数字签名的作用：**

**1.接收者能够核实发送者的签名（不能冒充）**

**2.发送者事后不能否认**

**3.签名不能伪造、篡改**

48.数字签名的流程

**在实际的应用中，数字签名的流程如下：**

**1.用Hash算法对消息进行运算，生成消息摘要。**

**2.对1中生成的消息摘要使用发送者的私钥进行加密，得到数字签名。**

**3.将消息+Hash算法（生成消息摘要）+数字签名一起发送给接收者。**

**4.接收者使用相同的Hash验证接收的消息是否被修改，之后使用发送者的公钥来解密签名验证是否是发送者发送的。**

第9章 PKI技术

49.什么是数字证书？

**数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。**

50.在信任链条中，CA的作用是什么？

**仲裁、颁发数字证书等工作**

51.数字证书的格式是哪个标准规定的？

**X.509**

第12章 Web安全

52.HTTPS可以简单的理解为什么？

**HTTPS简单地说，就是HTTP + SSL/TLS。**

53.SSL协议栈中有哪些协议？哪个协议是用来建立安全通道的？哪个协议在最底层？

**SSL握手协议、SSL更改密码协议、SSL警告协议、SSL记录协议。SSL握手协议。SSL记录协议。**

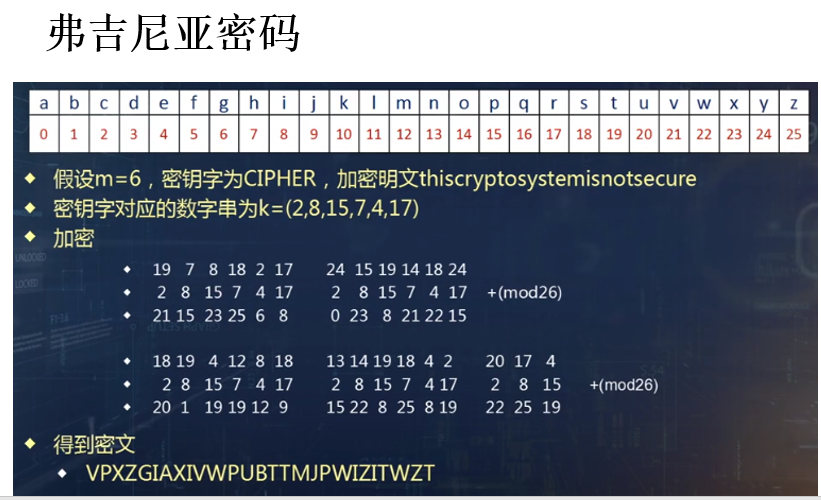
计算题样例：

1.已知：加密方案为凯撒密码加密，密钥key=3，明文为：avengers，求：对应的密文（或已知密文求明文，p.55-习题1）。

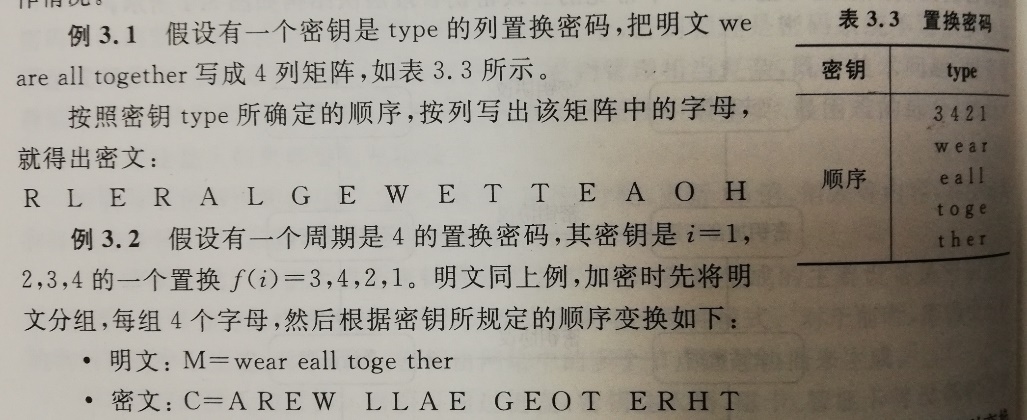


2、已知：加密方案为弗吉尼亚密码（字母编码表见下图），密钥：dlnu，明文为ilovechina，求对应的密文（或已知密文求明文）。。

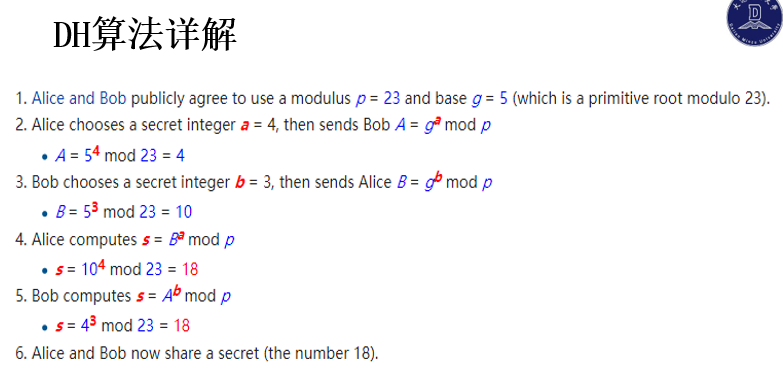




3、已知：加密方案为列置换加密，已知明文求密文或已知密文求明文（p.48-例3.1）



4、在Diffie-Hellman秘钥交换协议中，选定Alice和Bob双方协商的公共素数为：p=23,q=5, Alice的私钥是keya=4,Bob的私钥是keyb=3，则他们互相交换的公钥pa和pb分别是多少？他们共享的对称密钥是多少？要求：有计算过程。



5、在RSA算法中，选取的两个大素数为：p=7，q=17，请给出一对公钥和私钥，要求：有计算过程（p.101-习题5）。

