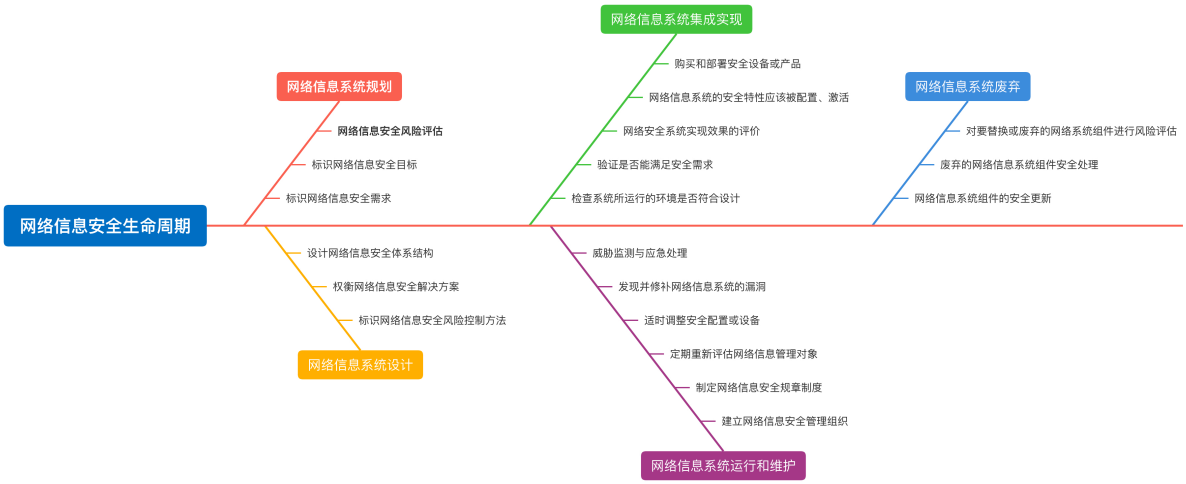
网络信息安全考点汇总

1.网络安全概述

- 网络安全的基本属性
  - 机密性（网络信息不泄露给非授权用户）
  - 完整性（网络信息或系统未经授权不能进行更改）
  - 可用性（合法许可用户能够及时获取网络信息或服务）
  - 抗抵赖性
  - 可控性
- 互联网域名安全管理
  - 域名系统出现网络与信息安全事件时，应当在**24小时内**向电信管理机构报告。
- 网络信息系统生命周期



2.网络攻击原理与常用方法

- 网络攻击模型 - 攻击树模型
  - 优点
    - 能够采取专家*头脑风暴法*，将意见融合到攻击树中
    - 能够进行费效分析或者概率分析
    - 能够建模非常复杂的攻击场景
  - 缺点
    - 不能建模多重尝试攻击、时间依赖及访问控制等场景
    - *不能建模循环事件*
    - 对于现实中的大规模网络处理过程复杂
- 网络攻击一般过程

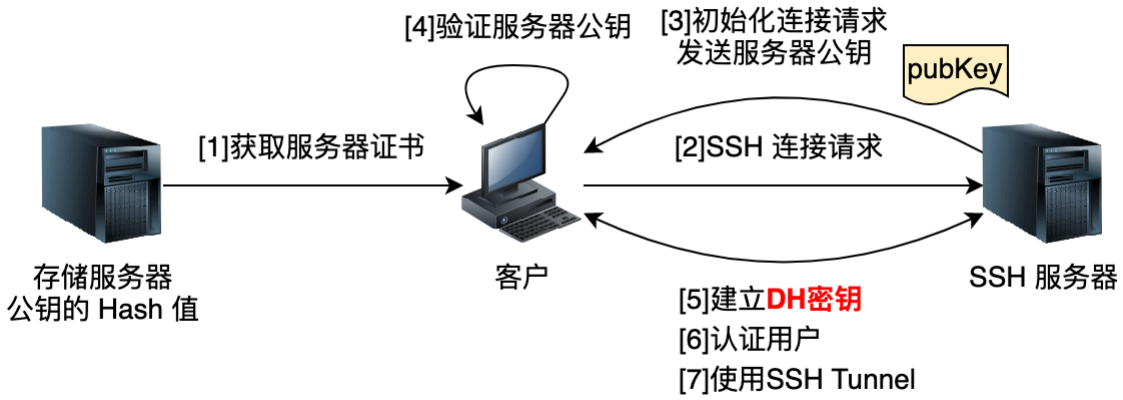
    - 隐藏攻击源
    - 收集攻击目标信息
    - 挖掘漏洞信息
    - 获取目标访问权限
    - 隐蔽攻击行为
    - 实施攻击
    - *开辟后门*
        - 放宽文件许可权
        - 重新开放不安全的服务
        - 替换系统本身的共享库文件
        - 修改系统的源代码
        - 安装各种特洛伊木马
        - 安装嗅探器
        - 建立隐蔽信道
    - 清除攻击痕迹
- 网络攻击常见技术方法 - 端口扫描
    - *完全连接扫描*：TCP/P 三次握手建立完整连接；
    - 半连接扫描：三次握手只完成前两次；
    - *SYN 扫描：发送连接请求，返回 ACK表示端口开放，返回 RST表示端口未开放*
    - *SYN/ACK 扫描：发送 SYN/ACK 数据包，返回 RST 端口未开发，未返回信息端口开放（被丢弃）；*
    - FIN 扫描：发送FIN数据包，返回 RST 说明端口关闭，未返回说明端口关闭；
    - ACK 扫描：发送FIN数据包，返回数据包TTL小于64或WIN大于0，说明端口开放；
    - NULL 扫描：发送的数据包将ACK、FIN、RST等标志位全部置空，未返回说明端口开放，返回RST说明端口关闭；
    - XMAS 扫描：源主机发送的数据包将ACK、FIN、RST等标志位全部置1，未返回说明端口开放，返回RST说明端口关闭。
- 网络攻击常见技术方法 - 拒绝服务
    - *同步包风暴（SYN Flood）*：发送大量半连接状的服务请求，使Unix等服务主机无法处理正常的连接请求；
    - *UDP 洪水（UDP Flood）*： 利用简单的TCP/IP服务，如用Chargen和Echo传送毫无用处的占满带宽的数据；
    - *Smurf 攻击*： 回复地址设置成目标网络广播地址的ICMP应答请求数据包，使该网络的所有主机都对此ICMP应答请求作出应答，导致网络阻塞；或者将源地址改第三方的目标网络，最终导致第三方网络阻塞；
    - ***泪滴攻击（Teardrop Attack）*** ： 通过加入过多或不必要的*偏移量字段*，使计算机系统重组错乱，产生不可预期的后果，暴露出 IP 数据包分解与重组的弱点。

- 网络攻击常见技术方法 - 网络钓鱼
  - 通过**假冒可信方**（知名银行、在线零售商 信的品牌）提供网上服务，以欺骗手段获取敏感个人信息（如口令、信用卡详细信息等）。

3.密码学基本理论

- 密码分类
  - 核心密码
  - 普通密码
  - 商用密码
- 密码体制分类
  - 私钥密码体制（对称密码体制）
    - DES - 分组加密：每组 64bit，密钥 56bit，迭代 16 圈，*圈密钥 48bit*；
    - TDES - 三重DES：加密（DES Ek1）-- 解密（DES Dk2）--加密（DES Ek3）
    - IDEA - 分组加密：每组 64bit，密钥 128bit
    - AES - 分组加密：密钥 *128bit / 192bit / 256bit*
  - 公钥密码体制（非对称密码体制）
    - RSA
  - 混合密码体制
    1. 发送者用对称密钥对消息加密；
    2. 发送者用公钥对加密消息再加密，形成*数字信封*；
    3. 接收者用私钥解密数字信封；
    4. 接收者用对称密钥解密消息。
- 国密算法
  - *SM1 对称加密* 分组128比特，密钥128比特
  - SM2 非对称加密 基于椭圆曲线
  - ***SM3 杂凑算法*** 杂凑值长度256比特
  - *SM4 对称加密* 分组128比特，密钥128比特
  - SM9 标识密码算法
- Hash 算法：以下算法 ***分组长度均为 512 比特***，自上而下安全性逐渐增强！
  - MD5：哈希值 128 比特
  - SHA：哈希值 160 比特
  - ***SM3：哈希值 256 比特***
- 数字证书
  - 由证书认证机构（CA）签名，包含：
    - 公钥信息
    - 拥有者信息
    - 签发者信息

        - 签名算法
        - 有效期
- 安全协议 - SSH
    - 协议构成
        - *SSH传输层协议*：提供算法协商和密钥交换，并实现服务器的认证，形成加密的安全连接，提供完整性、保密性和压缩选项服务；
        - *SSH用户认证协议*：口令认证、公钥认证、主机认证等；
        - *SSH连接协议*：将认证连接分解为不同的并发逻辑通道，支持*注册会话隧道*和*TCP转发*，且能为这些通道提供流控服务及通道参数协商机制。
    - 工作机制



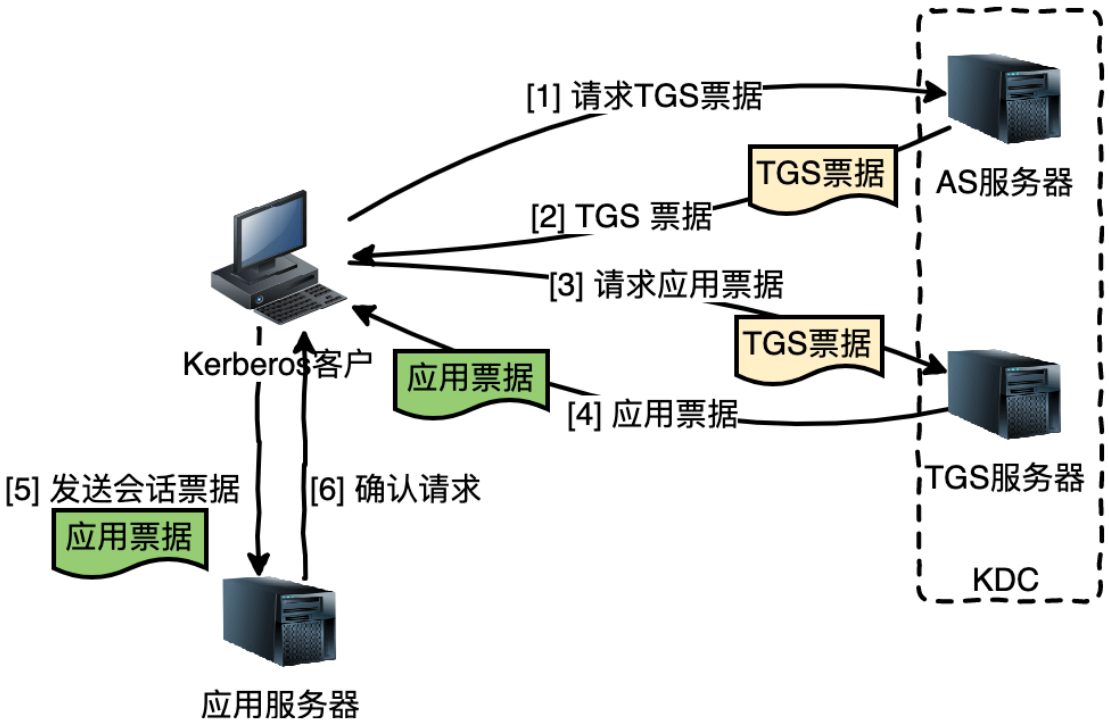
4.网络安全模型

- BLP 机密性模型 *（下读上写）*
    - *简单安全特性：* 主体对客体进行*读访问*的必要条件是*主体安全级 < 客体安全级*，主体的范畴集合包含客体的全部范畴，即主体***只能向下读，不能向上读***。
    - **特性：* 主体对客体进行*写访问*的必要条件是客体安全级支配主体的安全级，即*客体保密级 >= 主体保密级*，客体的范畴集合包含主体的全部范畴，即主体***只能向上写，不能向下写***。
- BiBa 完整性模型
    - *简单安全特性：* 主体对客体进行*修改访问*的必要条件是*主体完整性级别 >= 客体完整性级别*，主体的范畴集合包含客体的全部范畴，即主体***不能向下读*** ；
    - **特性：* 主体的完整性级别小于客体的完整性级别，不能修改客体，即主体***不能向上写***；
    - *调用特性：* 主体的完整性级别小于另一个主体的完整性级别，不能调用另一个主体。
- PDRR 模型
    - 保护：*信息隐藏*
    - 检测
    - 恢复

- 响应

5.认证技术

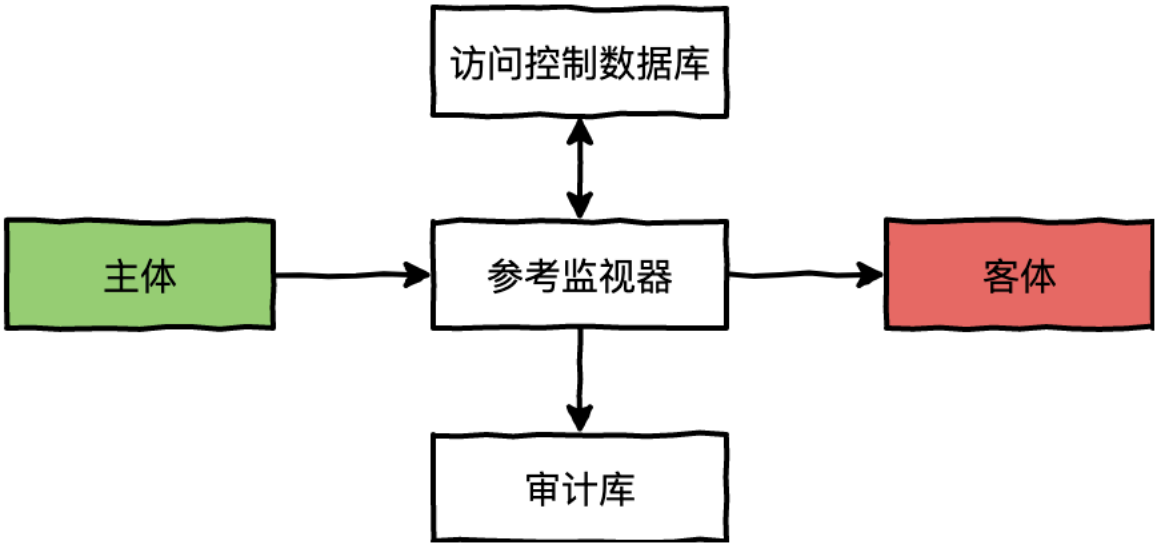
- 口令认证
  - *最常用的认证措施*
- 生物特征认证
  - 人脸、指纹、声音、虹膜、*DNA*
- Kerberos 认证
  - 利用对称加密（MD5），使用可信第三方位应用提供认证服务，在用户和服务器间建立安全信道；
  - 优点
    - 可以显著减少用户密钥的密文的暴露次数
    - 单点登录（SSO）
  - 缺点
    - 主机节点时间同步问题
    - 地域拒绝攻击服务
  - 认证过程



- 公钥基础设施技术（PKI）
  - 将实体和一个公钥绑定，并让其他的*实体（CA）* 能够验证这种绑定关系。
    - CA：证书授权机构，进行证书的颁发、废止和更新；
    - RA：证书登记机构，将公钥和证书持有者关联，进行注册和担保，辅助CA完成证书处理功能。

6.访问控制技术

- 访问控制模型
  - 主体
  - 客体
  - 参考监视器
  - 访问控制数据库
  - 审计库

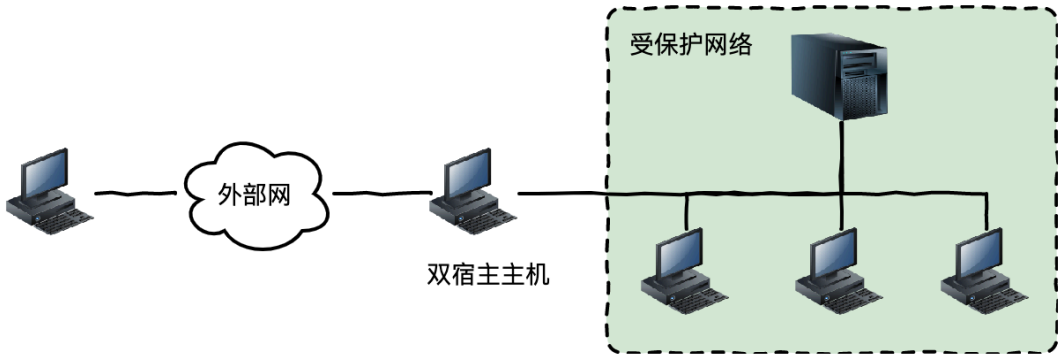


- 访问控制类型
  - 自主访问控制（DAC）
    - 基于行的自主访问控制
    - 基于列的自主访问控制
      - 保护位：以bit位表示所有者、所属组和其他客体的访问权限；
      - *访问控制表（ACL）*：每个客体附加一个主体明细表，表示*访问控制矩阵*。
  - 强制访问控制（MAC）
  - 基于角色的访问控制（RBAC）
  - 基于属性的访问控制（ABAC）

7.防火墙技术

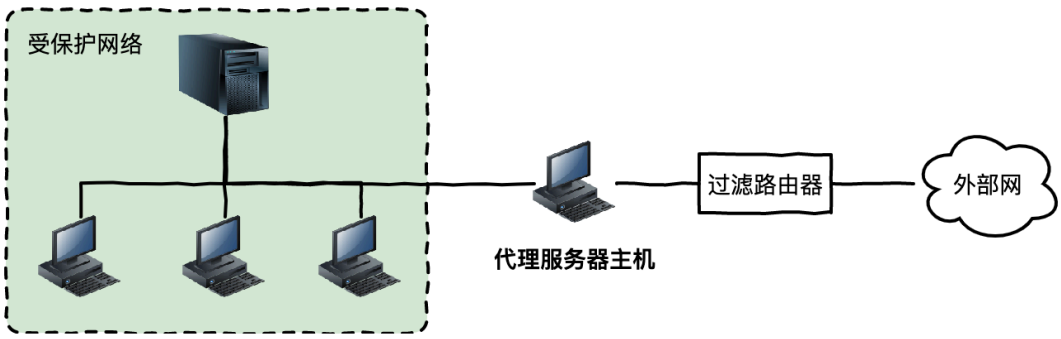
- 防火墙安全风险
  - 网络安全旁路
    - 只能对通过它的网络通信包进行访问控制，未通过它的无能为力
  - 防火墙功能缺陷
    - 不能完全防止感染病毒的软件或文件传输，需要在主机上安装反病毒软件
    - 不能防止基于数据驱动式的攻击

        - 不能完全防止后门攻击，例如 http tunnel
    - 防火墙安全机制形成单点故障和特权威胁
    - *防火墙无法有效防范内部威胁*
    - 防火墙效用受限于*安全规则*
- 包过滤规则 - *Cisco IOS*
    - 规则类型
        - 标准IP访问表：**access-list** list-number **{deny | permit} source** [source-wildcard] [**log**]
        - 扩展IP访问表：**access-list** list-number **{deny | permit}** protocol **source** [source-wildcard] source-qualifiers ***destination*** destination-wildcard destination-qualifiers [**log | log-input**]
    - 区别
        - 前者基于源地址；后者还可基于目的地址；
        - 前者 list-number 范围 1-99；后者 100-199；
    - 共同点
        - source-wildcard 表示发送数据包的主机 IP 地址的通配符掩码，1-“忽略”， 0-“需要匹配”，any-任何来源
        - destination-wildcard 表示接收数据包的主机 IP 地址的通配符掩码
        - log表示记录符合规则条件的网络包。
    - 示例
        - 禁止 tcp 协议的任何来源 IP 包访问 27665 端口：*access-list 170 deny any any eq 27665 log*
- 防火墙防御体系结构
    - 基于双宿主主机防火墙
        - 将内网和外网分别接在主机的**两张不同的网卡**上，二者之间需经过**安全检查模块**后才可通信。

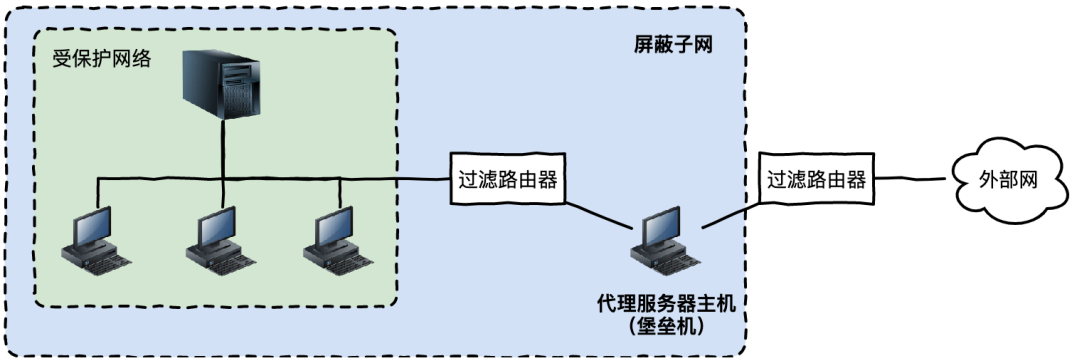


    - 基于代理型防火墙

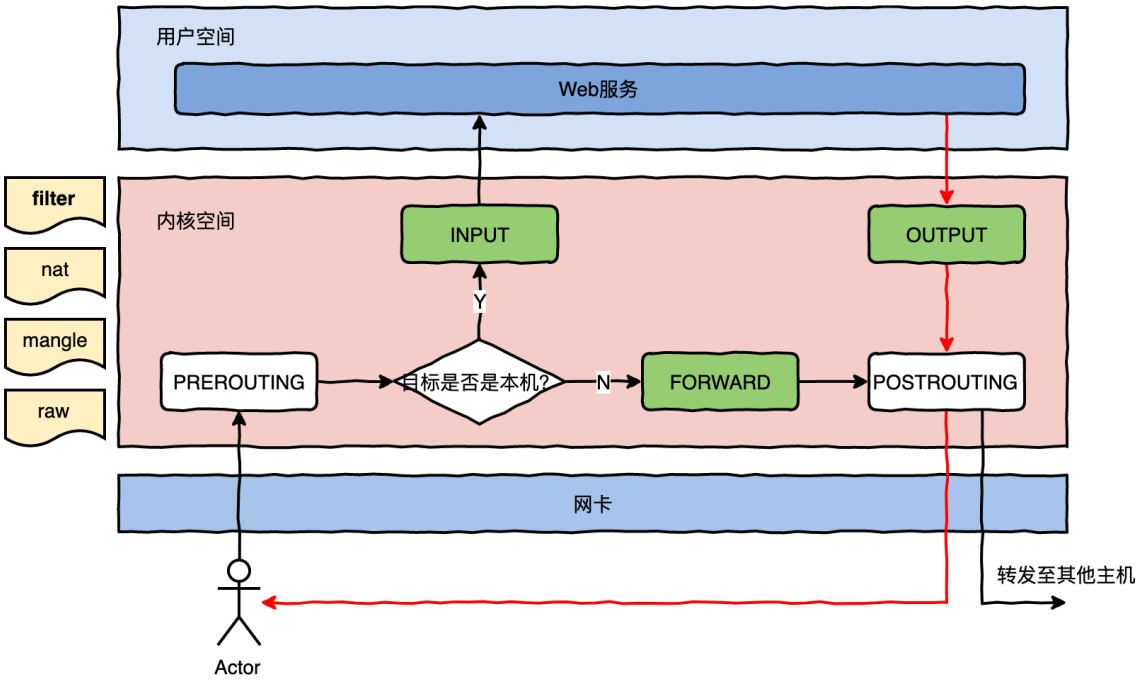
    - 由**代理服务器**和**路由器**构成，代理服务器位于内部网络，路由器按规则过滤数据包。



  - 基于屏蔽子网的防火墙
    - 在代理型结构中增加一层周边网络的安全机制，使内部网络和外部网络有两层隔离带。



- IPtables 防火墙
  - 原理

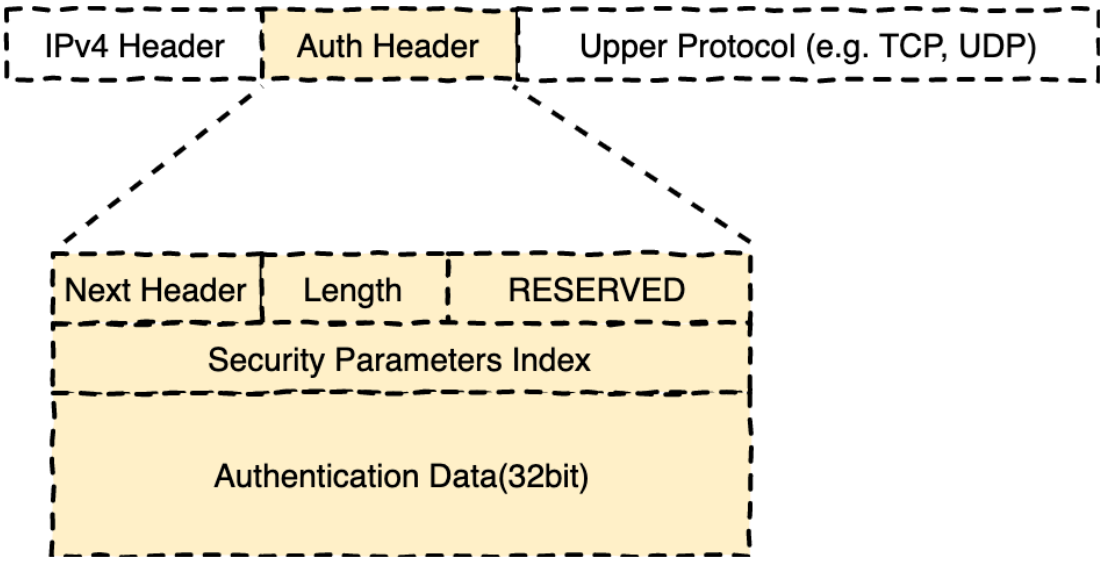


    - 规则
        - 查询表上所有链的所有规则
            - iptables -L
        - 为内置链设置默认策略
            - iptables -P INPUT DROP
            - iptables -P OUTPUT DROP
            - iptables -P FORWARD DROP
        - 禁用指定IP访问
            - iptables -A INPUT -s 196.16.x.y -j DROP
        - 允许外网访问
            - iptables -A INPUT -p tcp --dport 80,443 -j ACCEPT
        - 允许内网访问外网（ech1-外网，eth0-内网）
            - iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
        - 内网可以Ping外网
            - iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
            - iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
        - 外网可以Ping内网
            - iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
            - iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
        - 允许指定IP通过SSH访问
            - iptables -A INPUT -p tcp -s 192.16.xx.y -dport 22 -j ACCEPT
        - 对输入的HTTPS流量做负载均衡
            - iptables -A *PREROUTING* -p tcp --dport 443 *--every 3 --packet 0* -j *DNAT --to-destination* xxx.xx.x.1:443
            - iptables -A PREROUTING -p tcp --dport 443 --every 3 --packet 1 -j DNAT --to-destination xxx.xx.x.3:443
            - iptables -A PREROUTING -p tcp --dport 443 --every 3 --packet 2 -j DNAT --to-destination xxx.xx.x.3:443
- 地址转换技术（NAT）
    - 概念
        - 将内网地址转换为公网地址，解决了公网地址不足的问题，同时屏蔽了内网结构，提升内网安全性。
    - 分类
        - *静态 NAT （StaticNAT）*：内部网络中的每个主机都被*永久映射*成外部网络中的某个合法的地址。
        - *NAT池 （pooledNAT）*：在外部网络中配置合法*地址集*，采用*动态分配*的方法映射到内部网络。

        - *端口 NAT （PAT）*：把内部地址映射到外部网络的一个IP地址的*不同端口*上。
    - 应用
        - Linux 自带的 IPtables 防火墙技术。

8.VPN 技术

- VPN 安全服务
    - *保密性服务（Confidentiality）*：防止传输的信息被监听
    - *完整性服务（Integrity）*：防止传输的信息被修改
    - *认证服务（Authentication）*：提供用户和设备的访问认证，防止非法接入
- VPN 类型
    - *传输层 VPN*：SSL
    - *网络层 VPN*：受控路由过滤、隧道技术
    - *链路层 VPN*：ATM、Frame Relay、多协议标签交换MPLS
- VPN 实现技术 - IPSec（Internet Protocol Security）
    - IP AH（Authentication Header）
        - 作用：*保证IP包的完整性*和*提供数据源认证*，为IP数据报文提供无连接的完整性、数据源鉴别和抗重放攻击服务。
        - 原理：将IP包的部分内容用*加密算法*和*Hash算法*进行混合计算，生成一个完整性校验值，简称 *ICV（Integrity Check Value）*，同时把ICV附加在IP包中 。
    - IP ESP（Encapsulation Security Payload）
        - 作用：保证IP包的*保密性*
        - 原理：将IP包做加密处理，对整个IP包或IP的数据域进行安全封装，并生成带有ESP协议信息的IP包，然后将新的IP包发送到通信的接收方。
    - 密钥交换协议
        - 双方的安全关联的各种参数由 KDC（Key Distributed Center）和通信双方共同商定，共同商定的过程就必须遵循一个共同的协议，这就是密钥管理协议。
    - 两种传输模式
      - *透明模式（Transport Mode）*：只保护 IP 包中的数据域（data payload）；
      - *隧道模式（Tunnel Mode）*：保护IP包的包头和数据域。



- VPN 实现技术 - SSL
  - 握手协议：身份鉴别和安全参数协商
  - 密码规格变更协议：通知安全参数的变更
  - 报警协议：关闭通知和对错误进行报警
  - *记录层协议*：传输数据的分段、压缩及解压缩、加密及解密、完整性校验等

9.入侵检测技术

- 入侵检测模型 - CIDF模型
  - 事件产生器：从整个计算环境中获得事件，并向系统的其他部分提供事件。
  - *事件分析器*：分析所得到的数据，并产生分析结果。
  - 响应单元：对分析结果做出反应，如切断网络连接、改变文件属性、简单报警等应急响应。
  - 事件数据库：存放各种中间和最终数据，数据存放的形式既可以是复杂的数据库，也可以是简单的文本文件。
- 基于误用的入侵检测技术
  - 基于条件概论的误用检测方法
    - 将入侵方式对应一个事件序列，然后观测事件发生序列， 应用贝叶斯定理进行推理，推测入侵行为。
  - 基于状态迁移的误用检测方法
    - 利用状态图表示攻击特征，不同状态刻画了系统某一时刻的特征。 初始状态 危害状态
  - 基于键盘监控的误用检测方法
    - 假设入侵行为对应特定的击键序列模式，然后检测用户的击键模式，并将这一模式与入侵模式匹配，从而发现入侵行。
  - ***基于规则的误用检测方法 -- 开源项目 Snort***

        - 将攻击行为或入侵模式表示成一种规则，只要符合规则就认定它是一种入侵行为。
        - 优点：检测简单
        - 缺点：检测受到规则库限制，无法发现新的攻击，并且容易受干扰。
- 入侵检测系统
    - 基于主机的入侵检测系统（HIDS）-- SWATCH / Tripwire
    - ***基于网络的入侵检测系统（NIDS）*** -- Session Wall / Cisco Secure IDS / ***Snort***
      实际应用中通常将入侵检测系统放置在防火墙内部，可以*降低入侵检测系统的误报率*。
- 开源网络入侵检测系统 -- Snort
    - 原理：通过获取网络数据包，然后基于安全规则进行入侵检测，最后形成报警信息。
    - 安全规则：***alert*** *tcp* **any** **any** → 192.168.1.0/24 111 (***content*** : "| 00 01 86 a5 |"; ***msg*** : "mountd access";)
      其中，action 有：alert、log、pass、activate、dynamic

10.网络物理隔离技术

- 网闸
    - 利用GAP技术使两个或者两个以上的网络在不连通的情况下，实现它们之间的安全数据交换和共享。
    - 使用一个具有控制功能的开关读写存储安全设备，通过开关的设置来连接或切断两个独立主机系统的数据交换。

11.网络安全审计技术

- 网络审计数据保护技术
    - 系统用户分权管理：操作员、安全员、审计员；
    - 审计数据强制访问：对审计数据设置*安全标记*，防止非授权用户查数据；
    - 审计数据加密
    - 审计数据隐私保护
    - 审计数据完整性保护

12.网络安全漏洞防护技术

- 重大安全事件统计
    - Internet蠕虫：Sendmail 及 finger 漏洞
    - 分布式拒绝服务攻击：TCP/IP 协议漏洞
    - “红色代码”蠕虫：微软 Web 服务器 IIS 4.0或5.0中 index 服务的安全漏洞
    - Slammer蠕虫：微软MS SQL 数据库系统漏洞
    - 冲击波蠕虫：微软操作系统 DCOM RPC 缓冲区溢出漏洞
    - 震网病毒：Windows 操作系统、WinCC 系统漏洞

    - Wannacry勒索病毒：Windows 系统的 SMB 漏洞
- 网络安全漏洞来源
    - 非技术性安全漏洞
        - 网络安全责任主体不明确
        - 网络安全策略不完备
        - 网络安全操作技能不足
        - 网络安全监督缺失
        - 网络安全特权控制不完备
    - 技术性安全漏洞
        - *设计错误（Design Error）*
        - 输入验证错误（Input Validation Error）
        - *缓冲区溢出 （Buffer Overflow）*
        - 意外情况处置错误（Exceptional Condition Handling Error）
        - 访问验证错误（Access Validation Error）
        - *配置错误（Configuration Error）*
        - 竞争条件（Race Condition）
        - 环境错误（Condition Error）

13.恶意代码防范技术

- 恶意代码分类
    - 主动传播 ***（具有自我复制和传播能力、可独立自动运行）***
        - *网络蠕虫*
    - 被动传播
        - 计算机病毒
        - 特洛伊木马
        - 间谍软件
        - 逻辑炸弹
- 计算机病毒特性
    - *隐蔽性*：计算机病毒附加在正常软件或文档中，例如可执行程序、电子邮件、Word 文档等，一旦用户未察觉，病毒就触发执行，潜入到受害用户的计算机中。
    - *传染性*：计算机病毒可以进行自我复制，并把复制的病毒附加到无病毒的程序中，或者去*替换磁盘引导区的记录*，使得附加了病毒的程序或者磁盘变成了新的病毒源，又能进行病毒复制，重复原先的传染过程。
    - *潜伏性*：计算机病毒感染正常的计算机之后，一般不会立即发作，而是等到触发条件满足时，才执行病毒的恶意功能，从而产生破坏作用。
    - *破坏性*：计算机病毒对系统的危害性程度，取决于病毒设计者的设计意图。
- 网络蠕虫扫描技术

    - *随机扫描*：网络蠕虫会对整个 IP 地址空间随机抽取的一个地址进行扫描，这样网络蠕虫感染下一个目标具有非确定性 -- ***Slammer*、*Lion Worm***
    - *顺序扫描*：网络蠕虫根据感染主机的地址信息，按照本地优先原则，选择它所在网络内的IP地址进行传播 -- ***Blaster*（*也支持随机扫描*）**
    - *选择性扫描*：网络蠕虫在事先获知一定信息的条件下，有选择地搜索下一个感染日标主机 -- ***CodeRed*、*震荡波*（*也支持随机扫描*）**
- 僵尸网络
    - 指攻击者利用入侵手段将***僵尸程序***（bot or zombie）植入目标计算机上，进而操纵受害机执行恶意活动的网络。

14.网络安全主动防御技术

- 蜜罐主机技术
    - *空系统* 标准机器，上面运行着真实完整的操作系统及应用程序。在空系统中可以找到真实系统中存在的各种漏洞，与真实系统没有实质区别。
    - *镜像系统* 安装的操作系统、应用软件以及具体的配置与真实的服务器基本一致。
    - *虚拟系统* 一台真实的物理机上运行一些仿真软件，通过仿真软件对 计算机硬件进行模拟，使得在仿真平台上可以运行多个不同的操作系统，这样一台真实的机器就变成了多台主机（称为虚拟机）。 *-- Honeyd：专用的虚拟蜜罐系统构建软件*
- 隐私保护技术
    - 抑制 将数据置空的方式限制数据发布。
    - *泛化* 降低数据精度来提供匿名。
    - 置换 改变数据的属主。
    - 扰动 在数据发布时添加一定的噪声，包括数据增删、变换等，使攻击者无法区分真实数据和噪声数据，从而对攻击者造成干扰。
    - 裁剪 将敏感数据分开发布。

15.网络安全风险评估技术

- 网络安全风险评估过程
    - 评估准备
        - 确定评估对象和范围 → 生成评估文档
    - *资产识别*
        - 网络资产鉴定：*网络设备、主机、服务器、应用、数据和文档资产*
        - 网络资产价值估算
            - 以资产的三个基本安全属性为基础衡量：保密性、完整性和可用性，是*相对价值*；
            - 国家信息风险评估标准将资产价值分为*五级*。
    - 威胁识别
    - 脆弱性识别

- *已有安全措施确认*
- 风险分析
- 风险处理与管理

16.网络安全测评技术

- 网络安全测评分类 -- 基于实施方式
  - *安全功能检测* 对信息系统的安全功能实现状况进行评估，检查安全功能是否满足目标和设计要求
  - 安全管理检测
  - 代码安全审查
  - 安全渗透
  - 信息系统攻击测试
- 网络安全渗透测试流程 -- 五个阶段
  - *受理*：用户确认渗透性目标
  - *准备*：签订授权书及撰写测试方案
  - *实施*：确认渗透时间，执行渗透方案；
  - *综合评估*：汇总分析渗透数据，验证安全威胁场景及安全影响；
  - *结题*：撰写渗透分析报告及安全改进建议。

17.操作系统安全保护

- Windows 审计日志：记录系统运行情况，目录 *system32\config*
  - 系统日志 -- *SysEvent.evt*
  - 应用程序日志 -- *AppEvent.evt*
  - 安全日志（只允许系统管理员访问）-- *SecEvent.evt*
- Windows 系统安全增强技术 - 如何配置安全策略?
  - 密码复杂度要求
  - 账户锁定阈值
  - 账户锁定时间
  - 账户锁定记数器
    有关系统的安全设置规则，在 Windows 系统中需要配置的安全策略主要有账户策略、审计策略、远程访问、文件共享等。

18.数据库系统安全

- Oracle 数据库账户密码安全隐患
  - *Oracle 内部密码，储存在stXXX.cmd文件中*，其中 XXX是 Oracle 系统 ID 和SID， 默认是“ORCL”。这个密码用于数据库启动进程，提供完全访问数据库资源。这个文件在 Windows NT 中需要设置权限。

- *Oracle 监听进程密码，保存在文件“listener.ora”中*，保存着所有的 Oracle 执行密码，用于启动和停止Oracle 的监听进程。这就需要设置一个健壮的密码来代替默认的， 并且必须对访问设置权限。入侵者可以通过这个弱点进行 DoS 攻击。
- *Oracle 的“orapw”文件权限控制*，Oracle 内部密码和账号密码允许 SYSDBA 角色保存在“orapw”文本文件中，该文件的访问权限应该被限制。即使加密，也能被入侵者暴力破解。

19.网络设备安全

- 交换机分类
  - *第一代交换机 -- 集线器 -- OSI物理层*
    - 对接收到的信号进行再生整形放大，延长网络通信线路的 传播距离，同时，把网络中的节点汇聚到集线器的一个中心节点上。集线器会把收到的报文向所有端口转发。
  - *第二代交换机 -- 以太网交换机 -- OSI数据链路层*
    - 识别数据中的 MAC 地址信息，并根据 MAC地址选择转发端口。
  - *第三代交换机 -- 三层交换机 -- OSI网络层*
    - 针对 ARP/DHCP 等广播报文对终端和交换机的影响，***通过虚拟网络（VLAN）技术来抑制广播风暴***，将不同用户划分为不同的VLAN，VLAN之间的数据包转发通过交换机内置的硬件路由查找功能完成。
  - *第四代交换机 -- 三层交换机 -- OSI网络层*
    - 新增防火墙、负载均衡、IPS等功能，通常由多核CPU实现。
  - *第五代交换机 -- 三层交换机 -- OSI网络层*
    - 通常支持软件定义网络（SDN），具有强大的QoS能力。
- 网络设备安全机制 - 访问控制方法
  - *CON端口访问* 指定 X.Y.X.1 可以访问路由器
    - access-list 1 permit X.Y.X.1
    - access-class 1 in
  - *VTY 访问控制* 指定IP X.Y.Z.12/X.Y.Z.5 可以访问路由器
    - access-list 10 permit X.Y.Z.12
    - access-list 10 permit X.Y.Z.5
    - access-list 10 deny any
    - line vty 0 4
    - access-class 10 in
  - *HTTP 访问控制* 限制指定IP 地址可以访问网络设备
    - access-list 20 permit X.Y.Z.15
    - access-list 20 deny any
    - ip http access-class 20
  - ***SNMP 访问控制***

        - SNMIP访问认证
            - 设置只读 SNMP访问模式的社区字符串
                - snmp-server community UnGuessableStringReadOnly RO
            - 设置读/写 SNMP 访问模式的社区字符串
                - snmp-server community UnGuessableStringWriteable RW
        - 限制 SNMP访问的IP地址
            - 只有有X.Y.2.8和X.Y.2.7的IP 地址对路由器进行 SNMP只读访问
                - access-1ist 6 permit X.Y.Z.8
                - access-1ist 6 permit X.Y.Z.7
                - access-1ist 6 deny any
                - snmp-server comnunit UnGuessableStringReadOnly RO 6
        - 关闭SNIP访问
            - no snmp-server community UnGuessablestringReadonly RO
    - *设置管理专网*
        - 建立专用的网络管理设备，增强远程访问的安全性
        - 指定管理机器的IP才可以访问网络设备
            - 将管理主机和路由器之间的全部通信进行加密，使用 SSH 替换 Telnet。
            - 在路由器设置包过滤规则，只允许管理主机远程访问路由器。
    - *特权分级*
        - 交换机、路由器提供权限分级机制，每种权限级别对应不同的操作能力。
- 网络设备常见漏洞
    - 拒绝服务漏洞
    - 跨站伪造请求 CSRF （Cross-Site Request Forgery）
    - 格式化字符串漏洞
    - XSS（Cross—Site Scripting 代码执行（Code Execution）
        - CVE-2000-0945 信息显示思科 Catalyst 3500 XL 交换机的 Web 配置接口允许远程攻击者不需要认证就执行任意命令。
    - 溢出（Overflow）
        - 该类漏洞利用后可以导致拒绝服务、特权或安全旁路。
        - CVE-2006-4650漏洞信息显示，Cisco IOS 12.0、12.1、12.2处理GRE IP 不当，存在整数溢出，攻击者可以注入 构造特包到路由队列，从而引发路由 ACL 被旁路。
    - 内存破坏（Memory Comuption）
        - 会对路由器形成拒绝服务攻击。
        - CVE-2010-0576 漏洞信息显示，Cisco IOS 12.4 对 MPLS包处理不当，导致攻击者远程构造恶意包干扰思科相关的网络设备的运行，形成拒绝服务。

20.网络安全需求分析

- 网络安全等级保护体系 -- 五个保护等级 （《信息安全技术网络安全等级保护测评要求》规定）
  - 1 - 用户自主保护级
  - 2 - 系统保护审计级 -- *政务网站原则上不低于二级，2年测评一次*
  - 3 - 安全标记保护级 -- 每年测评
  - 4 - 结构化保护级
  - 5 - 访问验证保护级

21.云计算安全

- 云计算技术新增安全需求
  - 多租户安全隔离
  - 虚拟资源安全
  - 云服务安全合规
  - 数据可信托管
  - 安全运维
  - 连续性保障
  - 隐私保护

综合分析题

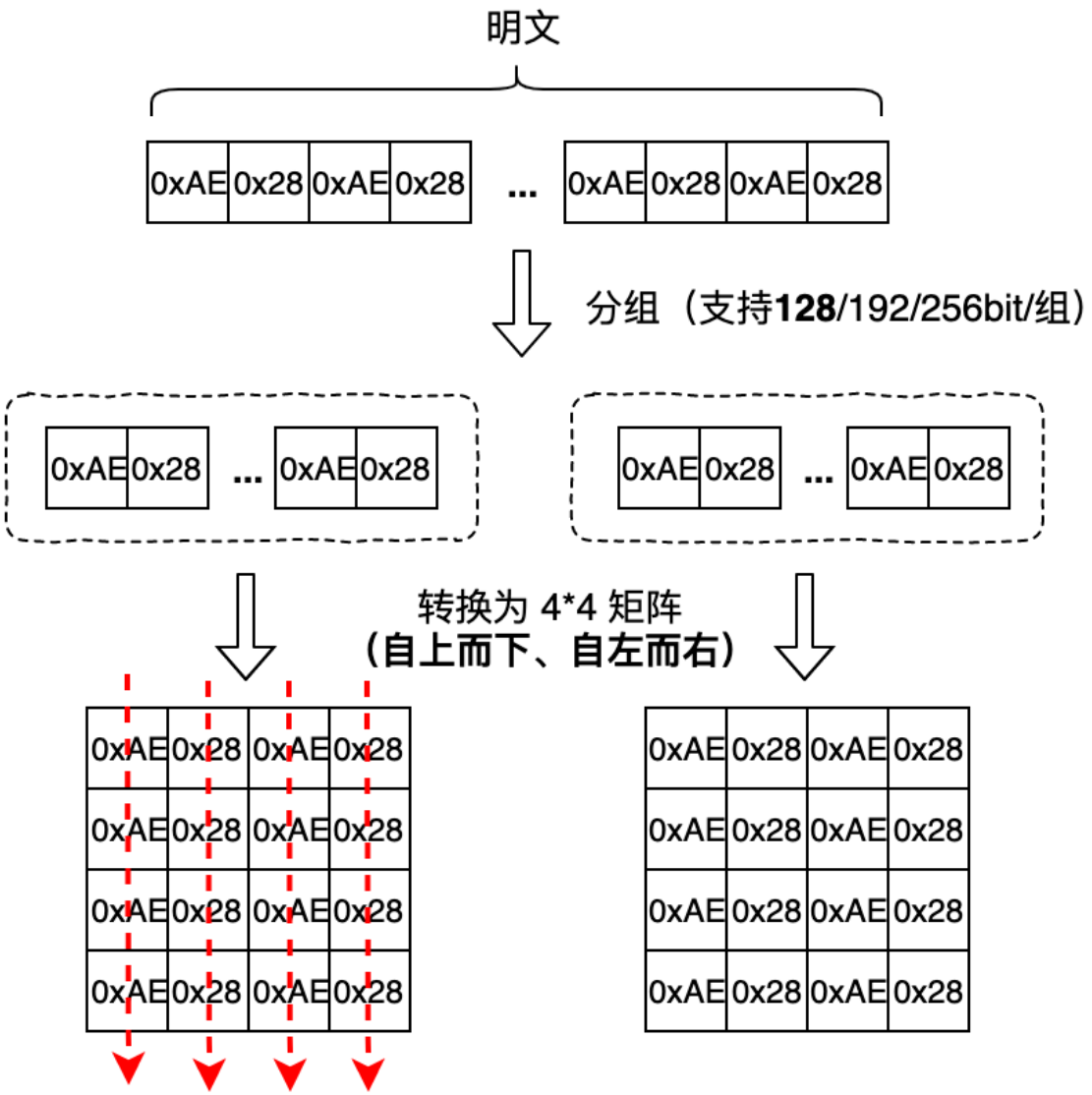
一、加密算法

DES

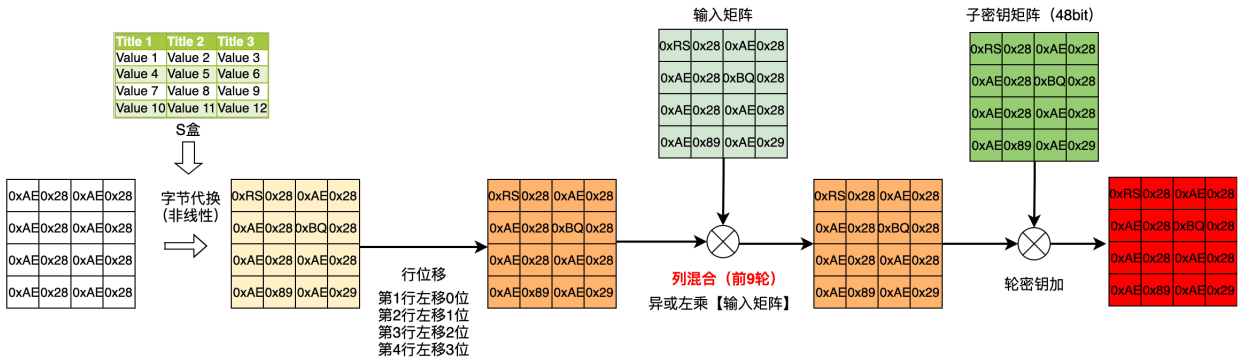
AES

分为两个阶段：初始变换和循环运算。

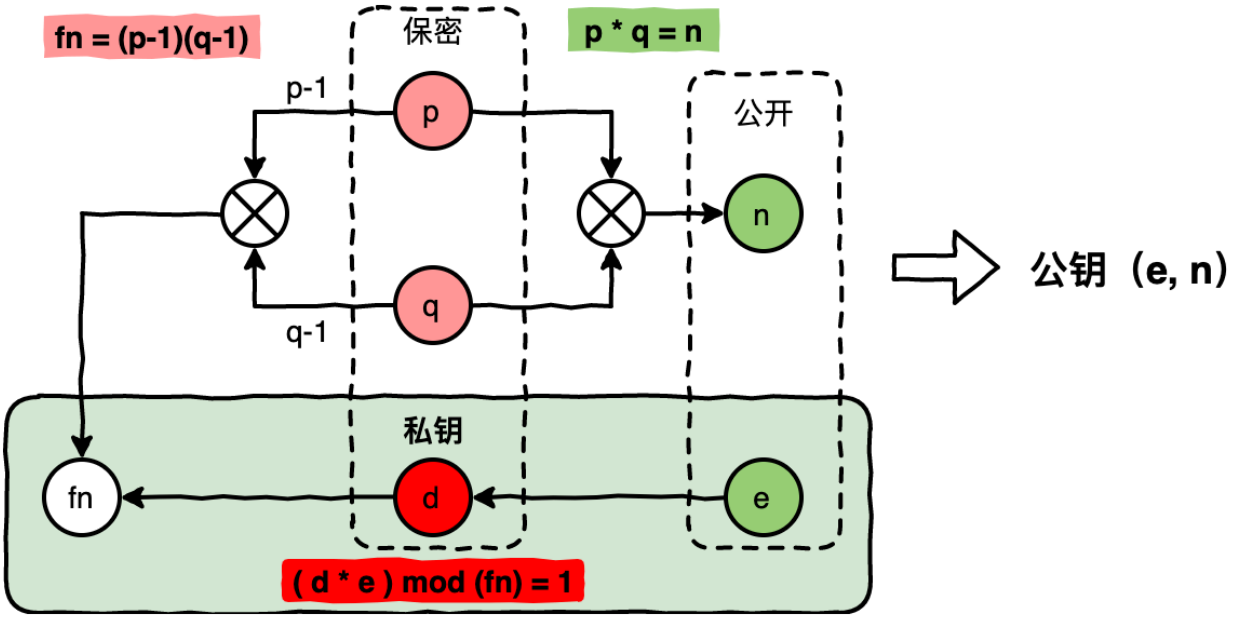
1. 初始变换


明文
0xAE 0x28 0xAE 0x28 ... 0xAE 0x28 0xAE 0x28
分组（支持128/192/256bit/组）
0xAE 0x28 ... 0xAE 0x28
0xAE 0x28 ... 0xAE 0x28
转换为 4*4 矩阵
（自上而下、自左而右）
0xAE 0x28 0xAE 0x28
0xAE 0x28 0xAE 0x28
0xAE 0x28 0xAE 0x28
0xAE 0x28 0xAE 0x28
0xAE 0x28 0xAE 0x28
0xAE 0x28 0xAE 0x28
0xAE 0x28 0xAE 0x28
0xAE 0x28 0xAE 0x28

2. 循环运算


Title 1 Title 2 Title 3
Value 1 Value 2 Value 3
Value 4 Value 5 Value 6
Value 7 Value 8 Value 9
Value 10 Value 11 Value 12
S盒
字节代换
（非线性）
行位移
第1行左移0位
第2行左移1位
第3行左移2位
第4行左移3位
输入矩阵
0xRS 0x28 0xAE 0x28
0xAE 0x28 0xBQ 0x28
0xAE 0x28 0xAE 0x28
0xAE 0x89 0xAE 0x29
列混合（前9轮）
异或左乘【输入矩阵】
子密钥矩阵（48bit）
0xRS 0x28 0xAE 0x28
0xAE 0x28 0xBQ 0x28
0xAE 0x28 0xAE 0x28
0xAE 0x89 0xAE 0x29
轮密钥加

RSA



二、Wireshark

- 如何通过数据包判断扫描源主机地址?
  - 通过端口判断：不同的请求，扫描源主机端口随机变化，而目的端口则是常见的80/443/22 等。
- 如何设置过滤条件?
  - *ip.src* eq 192.168.0.1 ***or/and*** *ip.dst* eq 192.168.0.2
  - *ip.addr* eq 192.168.0.3
  - *tcp.port* eq 80 / tcp.port == 80
  - *tcp.srcport* eq 80 / *tcp.dstport* eq 80
  - *frame.length* > 100
- 扫描类型?
  - 完全扫描类型
- *判断开放了哪些端口?*
  - 查看扫描的源主机与目的主机哪个端口建立了完整连接。如果没有回复（说明被丢弃）或者回复RST（关闭异常连接），说明端口未开放。
- TCP/IP基础：RST/ACK的标志字段为?
  - TCP头标志位顺序：[URG]*[ACK]*[PSH]*[RST][SYN][FIN]*
- iptables 如何阻止 wireshark 对目的主机扫描
  - iptables -A INPUT -p tcp -s 192.168.x.y -j DROP

三、计算机基础 - SSH

- SSH 服务默认工作端口?
  - 22
- 网络设备之间的远程运维可以采用两种安全通信方式?
  - SSH
  - VPN
- SSH 服务日志的位置?
  - */var/log/auth*
- Linux 系统默认不支持证书方式登录，要实现免密等了功能，需要修改哪个配置文件?
  - */etclssh/sshd_config*
- 完成 SSH 配置修改后，如何重启 SSH 服务?
  - systemctl restart ssh
- 配置完成后，如何清除历史操作记录?
  - *rm ~/.bash_history*

四、计算机基础 - UNIX/Linux 访问控制

- 一般通过文件*访问控制列表 ACL* 来实现系统资源的控制，也就是常说的通过“9bit”位来实现。

- 文件类型
  - b -- 块设备，存储数据的接口设备，例如硬盘
  - c -- 字符串口设备，例如键盘、鼠标等
  - l -- 链接文件，相当于windows的快捷方式
    - 创建软链：ln -s（指源文件source为绝对路径） source target
    - 列出 /home 下的所有软链：find /home *-xtype* l
    - 删除失效链接：find /home *-xtype l -delete*
  - s -- 套接字文件，用于进程间通信
  - d -- 目录
  -
    - -- 普通文件
- 9bit ACL

    - 前 3 bit -- 用户权限
    - 中 3 bit -- 用户组权限
    - 后 3 bit -- 其他用户权限
- 修改权限
    - chmod [***{ugoa}***{+-=}{rwx}] file
        - u -- 文件拥有者
        - g -- 文件所属组
        - o -- 其他人
        - a -- 所有人
    - chmod [777] file

五、Android 系统安全

- Android 系统结构以及对应的安全措施?
    - 应用程序层
        - 权限声明机制（*配置文件位置：AndroidManifest.xml*）
    - 应用框架层
        - 应用程序签名机制：Android 将应用程序打包成 *.APK文件*，应用程序签名机制规定对 APK 文件进行*数字签名*， 用来标识应用程序的*开发者*和*应用程序*之间存在信任关系。
    - 系统运行程序层
        - *安全沙箱*：**应用程序**和其相应运行的**Dalvik虚拟机**都运行在独立的Linux进程空间， 不与其他应用程序交叉，实现**完全隔离**。每个App和系统进程都被分配唯一固定的**UID**，与内核层进程的UID对应。每个App在各自独立的Dalvik虚拟机中运行，拥有独立的地址空间和资源。
        - SSL
    - 内核层
        - 分区 -- system.img只读，不允许用户写入；data.img可读写，存放用户数据
        - *地址空间布局随机化* -- 防止内核攻击
        - 文件系统安全 -- Linux ACL权限控制机制
        - SELinux -- 防止内核级提权攻击
- Android 系统权限组?
    - CALENDAR
    - CAMERA
    - CONTACTS
    - *LOCATION*
    - MICROPHONE
    - *PHONE*
    - SENSORS

    - SMS
    - STORAGE
      导航类软件应该具备的最小权限：LOCATION、PHONE
- 打包后的 APK 文件内容?
    - 静态资源文件（assets）
    - 库文件（lib）
    - 签名文件（META-INF）
    - 编译资源文件（res）
    - 配置清单文件（AndroidManifest.xml）
    - 核心代码文件（classes.dex）
    - 资源映射文件（resources.arsc）
- APP应用层序框架层四大组件面临的威胁?
    - Activities -- 界面劫持攻击
    - Broadcast Receiver -- 短信拦截攻击
    - Services
    - Content Providers -- 目录遍历攻击
- Android 系统支持的数据存储方式?
    - SharedPreferences
    - 文件存储
    - SQLite 数据库
    - ContentProvider
    - 网络存储
- 语法基础

JS

```
// 其他应用要访问 com.demo.AService 服务，如何声明?
<user-permission android:name = 'com.demo.AService'>

// 指定权限等级
<permission android:protectionLevel=["normal" | "dangerous" |
"signature" | "knownSigner" | "signatureOrSystem"]/>

// Wear 在其位于另一进程内的上下文流中显示 activity
<activity android:allowEmbedded='true'/>

// activity 可由其他组件的组件启动
<activity android:exported='true'/>

// 系统是否可实例化 activity
<activity android:enabled='true'/>
```