西安电子科技大学 XIDIAN UNIVERSITY
计算机科学与技术学院 School of Computer Science and Technology
国家示范性软件学院 National Pilot School of Software Engineering

计算机安全导论

第9章
安全模型与实践

主讲人：张志为

二〇二四年秋季学期

提纲

PART 1 | 策略、模型与信任

PART 2 | 访问控制模型

PART 3 | 渗透测试

PART 4 | Kerberos

PART 5 | 安全存储

提纲

PART 1 | 策略、模型与信任

PART 2 | 访问控制模型

PART 3 | 渗透测试

PART 4 | Kerberos

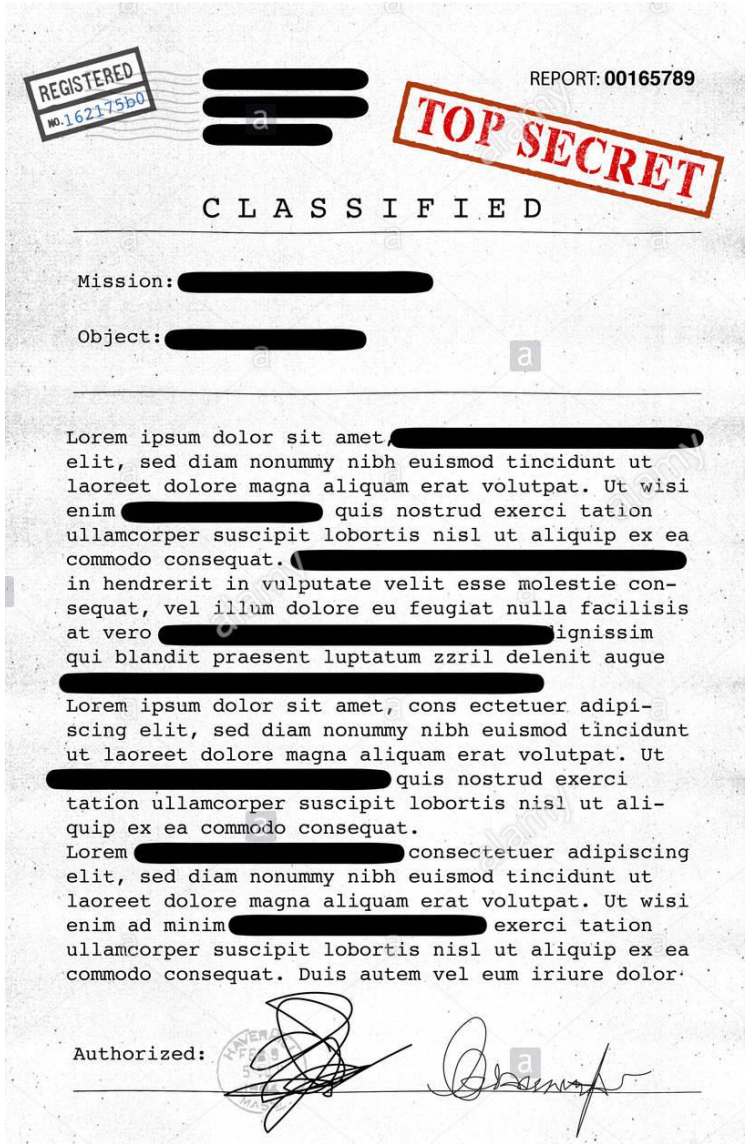
PART 5 | 安全存储

安全策略（5部分）

- **主体（Subject）**：与系统交互的代理，可以根据特定的个人定义，也可以根据个人群体在组织中可能持有的角色或级别来定义
  - 个人可以通过姓名或职称来识别，比如总裁、首席执行官或首席财务官。可以用术语来定义组，例如用户、管理员、将军、专业 、教员、院长、经理和行政助理。此类别还包括外部人员，如攻击者和来宾
- **客体（Object）**：客体是安全策略要保护和管理的信息与计算资源
  - 信息包括重要文档、文件与数据库，计算资源包括服务器、工作站和软件
- **动作（Action）**：主体对客体可能（或不可能）执行的操作
  - 操作一般包括文档的读取和写入、在web服务器上更新软件以及访问数据库的内容
- **权限（Permission）**：主体、操作与客体之间的映射，权限明确规定允许或禁止哪些操作
- **保护（Protection）**：策略中包含的特定安全特性或规则，以帮助实现特定的安全目标，如保密性、完整性、可用性或匿名性

安全模型

- **安全模型是一种抽象的、为管理员指定安全策略提供概念语言**
  - 通常，安全模型定义了组织成员所拥有的访问或修改权限的层次结构，因此，基于层次结构中这些权限所在的位置，就能轻松地对组织中的主体进行授权
  - 例如，军事文档的访问权限等级分为：不保密（unclassified），秘密（confidential），机密（secret），绝密（top - secret）



访问控制模型

自主访问控制（Discretionary Access Control）

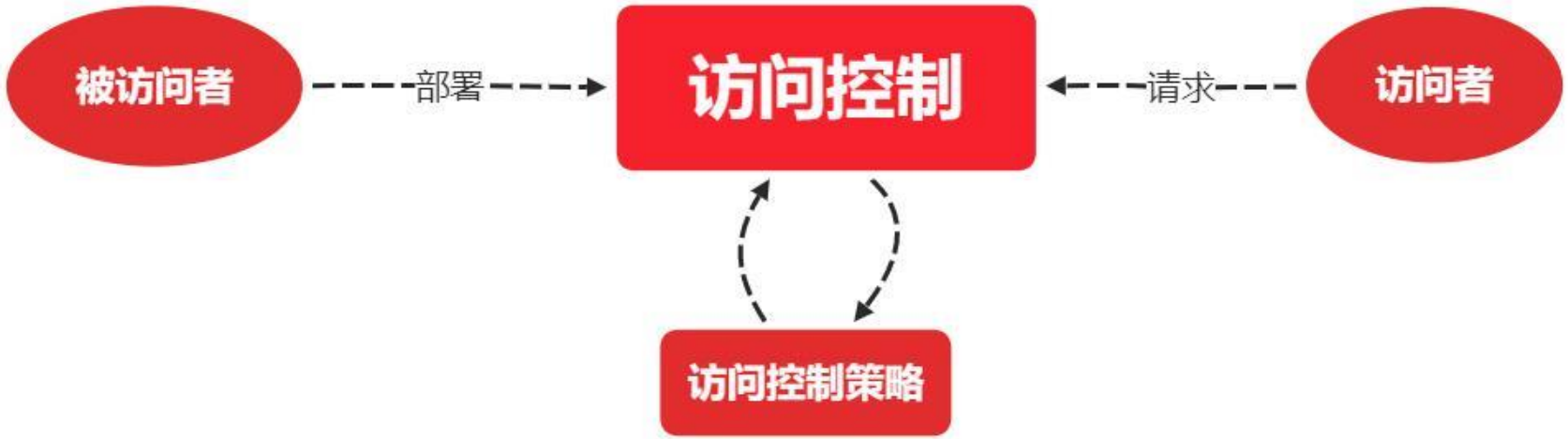
- 自主访问控制（DAC）指的是赋予用户能力确定文件访问权限的一种方案
- DAC通常具有用户和组的概念，并允许用户根据这些类别设置访问控制措施
- DAC方案还允许用户将资源特权授予同一系统上的其他用户

强制访问控制（Mandatory Access Control）

- MAC是一种限制性更强的方案，不管文件的所有权如何，它不允许用户定义文件的权限，而是由中央策略管理员制定安全策略。
- 每个安全规则都由主体（subject）、客体（object）和一系列的权限组成，其中主体表示试图获得访问权限的一方，客体是指被访问的资源，一系列权限定义了可以访问哪类资源

访问控制模型

- **自主访问控制 DAC** 的特点是客体的创建者可以授予其他主体对客体的访问权限，实现方式有访问控制矩阵、访问控制列表、访问控制能力列表
- **强访问控制 MAC** 是一种基于安全级别的访问控制，每一个主体和客体都被授予了不同的安全级别，通过判断主客体之间的安全级别进行访问控制

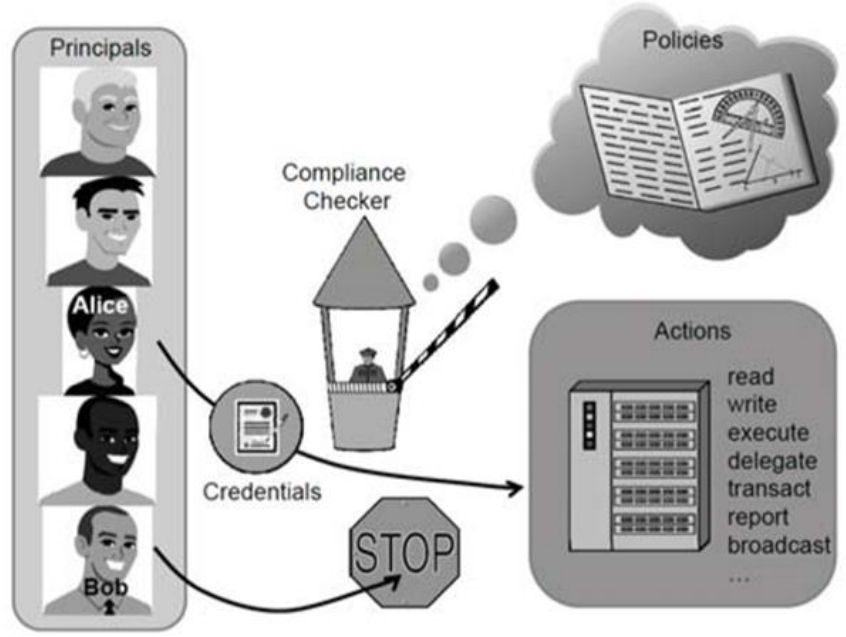


访问控制模型

- BLP模型，低安全级不可以向高安全级读，高安全级可以向低安全级读；低安全级可以向高安全级写，高安全级不可以向低安全级写
- Biba模型，低安全级不可以向高安全级写，高安全级可以向低安全级写；低安全级可以向高安全级读，高安全级不可以向低安全级读
- Chinese Wall中国长城模型，若干有竞争关系数据集构成了利益冲突类，同一个域里面的不同角色不能赋予相同的权限
- 基于角色的访问控制RBAC，不直接对用户授予权限，而是给用户赋予不同的角色，每个角色有不同的权限，基于角色的访问控制可能带来角色爆炸的情况
- 基于属性的访问控制ABAC，每个用户携带自己的属性，包括主体属性，资源属性和环境属性来访问客体，授权引擎根据这些属性进行访问控制

信任管理Trust Management

- **信任（trust）**的概念很难定义，信任涉及对实体能力和意图的信心，但也有主观因素：包括对风险的承受能力和文化背景。因此，我们不是对信任进行正式的、严格的定义，而是分析与信任相关的概念。**信任管理系统**由两个主要组成部分组成：策略语言（policy language）、一致性检查器（compliance checker）。策略规则由策略语言指定，并由一致性检查器执行
- 信任管理系统通常有规则如下
  - 操作（Action）：与系统安全相关的结果
  - 主体（Principal）：可以在系统上执行操作的用户、进程或其他实体
  - 策略（Policy）：就是制定的规则，制定赋予主体哪些权限，能执行那些操作
  - 凭证（Credential）：数字签名的文件，将主体身份与允许的行为绑定，包括允许主体将权限委托给其他主体的权限



提纲

PART 1 | 策略、模型与信任

PART 2 | 访问控制模型

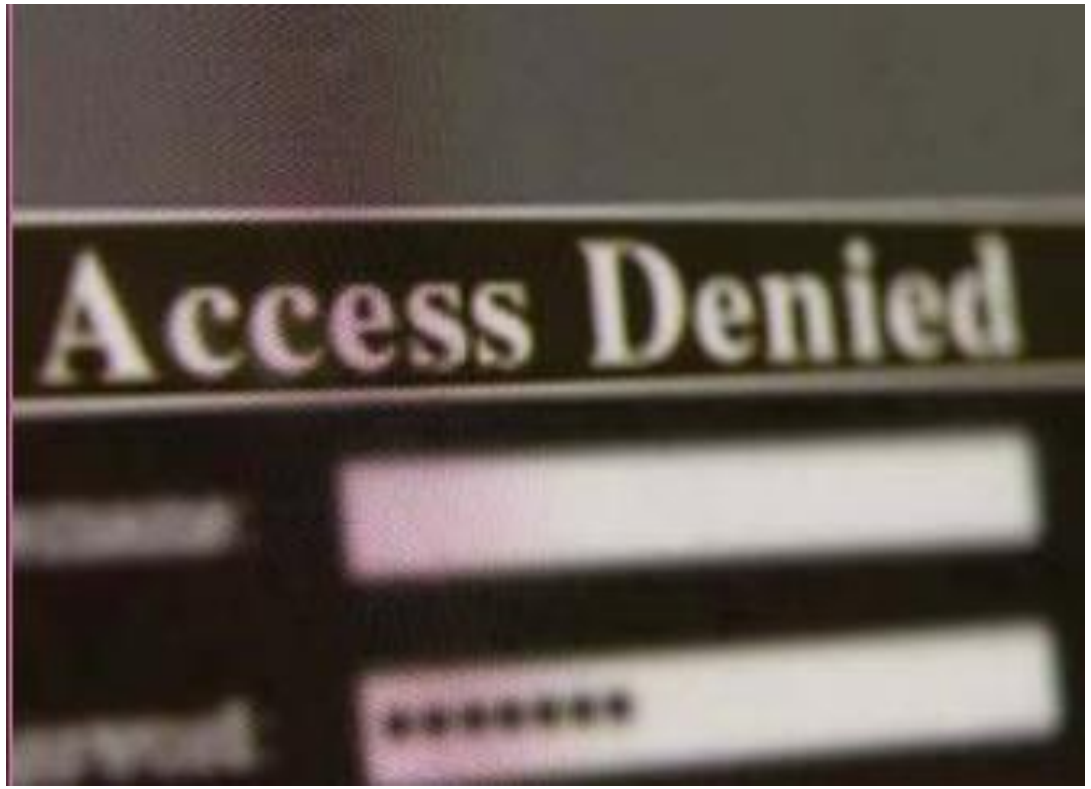
PART 3 | 渗透测试

PART 4 | Kerberos

PART 5 | 安全存储

访问控制模型

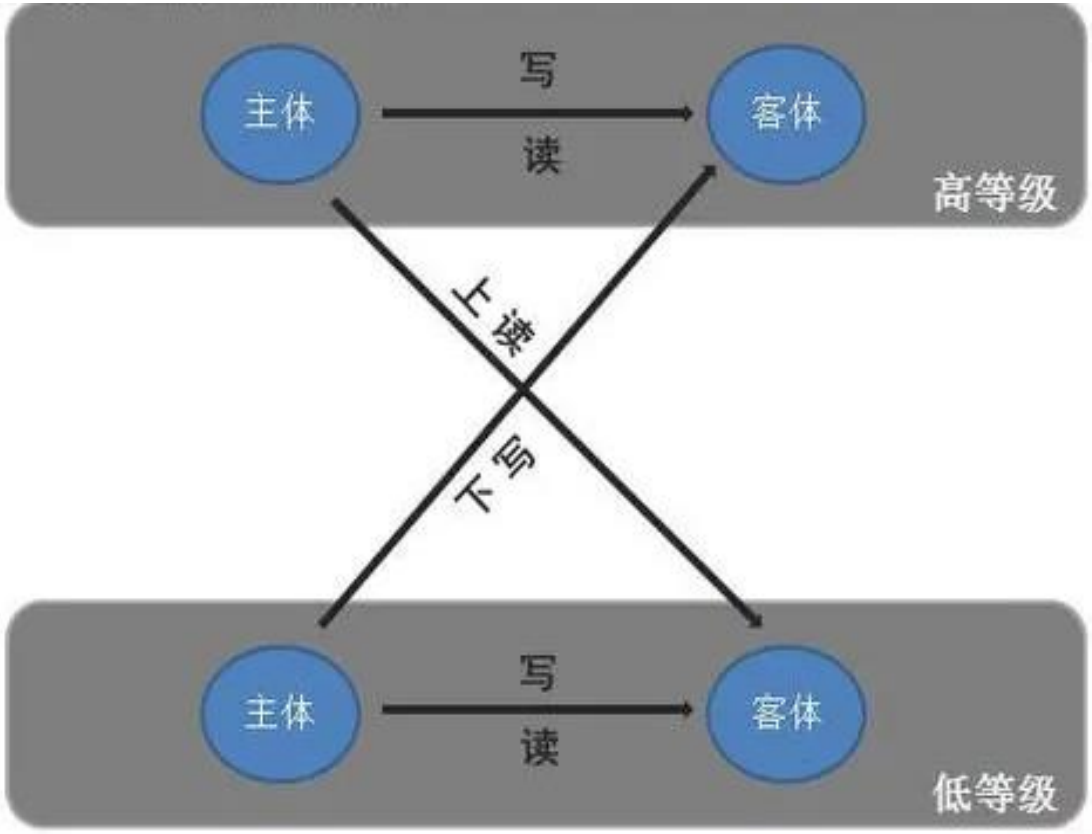
- 通过介绍各种已经被开发出来的模型，如何让通过正式化的机制，来保护存储在计算机系统中的文件的机密性和完整性
- 以下是几种常见的模型
  - Bell-La Padula(BLP)模型
  - Biba模型
  - 低水印模型
  - Clark-Wilson 模型
  - 中国墙模型(Brewer and Nash模型)



Bell-La Padula模型

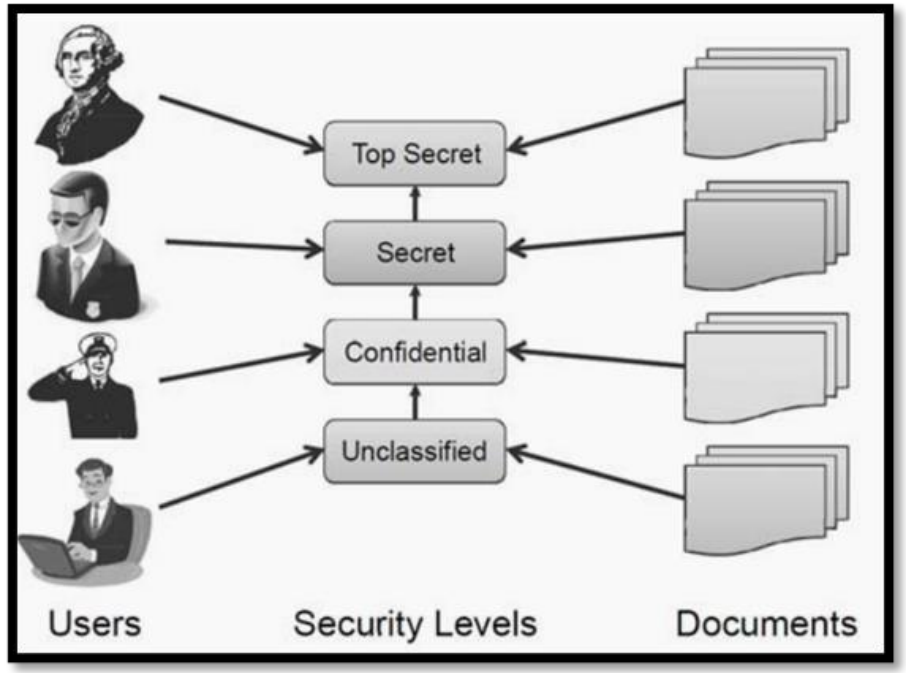
- Bell-La Padula模型是一个保护机密性的，强制访问控制模型的经典案例

- BLP模型源于军事**多级安全**（multilevel security）模式，传统上一直用于军事组织的文件分级和人员放行许可
- 这种模型在文档级别的安全性上具有严格的线性顺序，因此每个文档在这个顺序中都有一个特定的安全级别，并且每个用户都被分配了一个严格级别的访问，允许它们查看具有相应安全级别的所有文档



Bell-La Padula模型

- 军事分级层次结构
  - 系统有四种安全级别：最底层的是不保密unclassified、然后安全性呈升序的分别是秘密confidential、机密secret、绝密top - secret
  - 每个文件归类于一个安全级别
  - 每个用户都会在一个安全级别得到**放行许可**clearance
  - 只有具有相同或更高放行许可级别的用户才能访问对应安全级别的文件



Bell-La Padula模型

全序和偏序

- 在一个集合U上的一个**全序关系**（total order）应该满足以下性质:
  - 自反性（Reflexivity）：如果 x 在 U 中，则 $x \leq x$
  - 非对称性（Anti-symmetry）：如果 $x \leq y$ 且 $y \leq x$，则 $x = y$
  - 传递性（Transitivity）：如果 $x \leq y$，$y \leq z$，则 $x \leq z$
  - 完全性（Totality）：如果 x 和 y 在 U 中，则 $x \leq y$ 或 $y \leq x$
- 一般对于所有数（整数、实数）定义的“小于或等于”关系都是全序关系。
- 如果去掉完全性(Totality)，我们就得到了**偏序**(partial order)的概念，用符号“$\preccurlyeq$”表示

Bell-La Padula模型

BLP模型的工作原理

- 不同于军事模型中的严格的线性顺序，在BLP中形成的安全级别是偏序“≼”
- 每个对象 x 被分配到一个安全级别 L(X)。同样，每个用户 u 被分配到安全级别L(U)
- 用户对象的访问受以下两条规则控制：
  - **简单安全性质**（Simple Security Property）：只有满足如下条件，用户u才能读取对象x：

$$L(x) \preccurlyeq L(u)$$

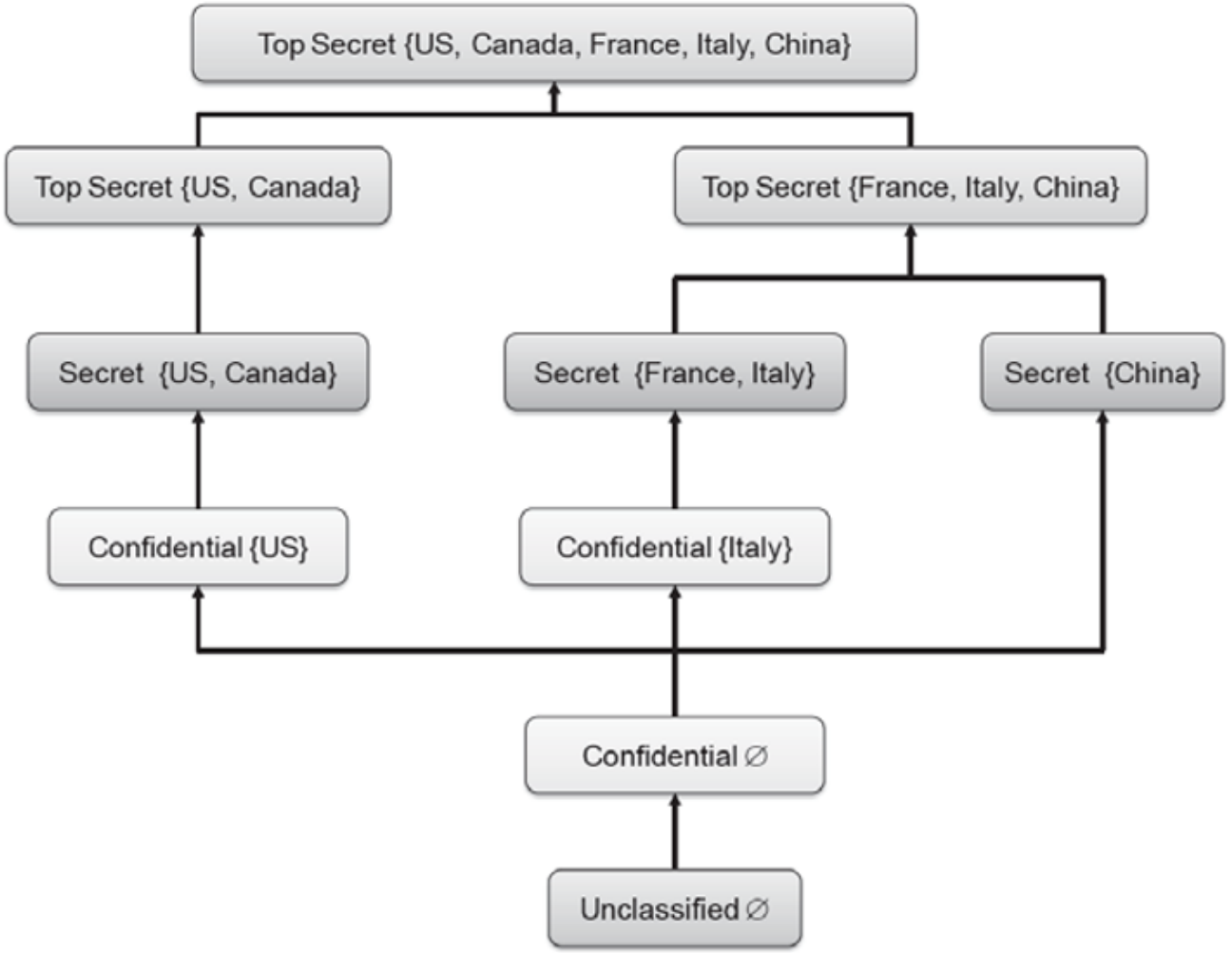
  - ***-性质**（*-property）只有满足如下条件，用户u才能写入（创建、编辑或追加）对象x：

$$L(u) \preccurlyeq L(x)$$

Bell-La Padula模型

- 简单安全性质也被称为“不可向上读”规则，因为它阻止用户查看安全级别高于自己的对象
- *-性质也称为“不可向下写”规则。它的目的是防止向安全性级别较低的用户传播信息
- BLP规则基于的原则是：**信息只能从低安全级别流向高安全级别**

- **使用分类定义安全级别**



其他的访问控制模型

Biba模型

- Biba模型的结构类似于BLP模型，但它解决的是完整性而不是保密性问题
- 为对象和用户分配的完整性级别（integrity levels）形成了偏序，与BLP模型类似
- Biba模型的完整性级别表明对象和用户的可信度或准确度，而不是确定保密级别
- Biba模型访问控制规则与BLP访问控制规则相反，也就是说，Biba不允许从下一级阅读，也不允许写到上层

其他的访问控制模型

Biba模型

- 如果让I(u)表示用户 u 的完整性级别，I(x)表示对象 x 的完整性级别，则Biba模型中有以下规则
  - 用户 u 只能在下列情况下读取对象x：

$$I(u) \preccurlyeq I(x)$$

  - 用户 u 只能在下列情况下才能写入(创建、编辑或追加)一个对象 x

$$I(x) \preccurlyeq I(u)$$

- 因此，Biba规则表达的原则是，**信息只能从较高的完整性级别下降到较低的完整性级别**

其他的访问控制模型

低水印模型（The Low-Watermark Model）

- 低水印模型是对Biba模型的扩展，它放宽了“不可向下读”的限制，但在其他方面类似于Biba模型
- 换句话说，**具有较高完整性级别的用户可以读取完整性级别较低的对象**
- 在这样的读取之后，对执行读取的用户进行降级，使其完整性级别与所读取对象的完整性级别相匹配

其他的访问控制模型

克拉克-威尔逊模型（The Clark-Wilson Model）

- 克拉克-威尔逊(CW)模型不处理文档机密性或完整性，而是处理执行事务的系统。CW模型的关键组件包括以下
  - 完整性约束：表明为了保证系统的状态有效，各对象之间必须满足的关系
  - 认证方法：验证事务给定的完整性约束。一旦认证了事务的程序，每次执行事务时，则不必再次进行完整性约束验证
  - 职责分离规则：防止执行事务的用户验证事务。通常，每个事务都被分配给可以分别验证和执行事务的不相交的用户集

其他的访问控制模型

中国墙模型（The Chinese Wall Model）

- 布鲁尔和纳什模式（通常被称为中国墙模式）被设计用于商业领域，以消除利益冲突的可能性
- 为了实现这一点，模型将资源分组为“利益冲突类” Conflict of Interest Classes
- 该模型执行这样的限制：每个用户只能从每个利益冲突类访问一个资源
  - 读规则：一、查看历史访问，若历史访问了某家公司的数据集，现在仍然可以访问；二、可以访问非利益冲突类，例如访问了A石油公司，还可以访问A银行，但是不能访问B石油公司。三、可以访问公开的信息
  - 写规则：现在要写的和之前读的都在同一个类中

基于角色的访问控制（Role-based Access Control）

- 基于角色的访问控制(RBAC)模型可以看作是文件系统中基于组的权限概念的演变

- **RBAC的优点**
  - 便于实现组织级的授权管理
  - 支持继承关系
  - 便于实现最小特权原则
  - 可实现职责隔离原则
  - 支持客体抽象；除了操作系统中提供的读、写以及执行权限之外，RBAC中可以根据实际应用的需要定义抽象的访问权限
  - 策略中立，通过不同配置能够实现特殊策略

基于角色的访问控制（Role-based Access Control）

RBAC的核心

- 用户（user）：用户是需要访问组织的资源以执行任务的实体。通常，用户是实际的人工用户，但用户也可以是机器或应用程序
- 角色（role）：角色定义为组织中具有类似功能和职责的用户的集合。大学中的角色可能包括“学生”“毕业生”“教师”“院长”“教职员”和“承包商”。一般来说，用户可能有多个角色
- 权限（permission）：权限描述了允许访问资源的方法。更具体地说，权限由对象执行的操作组成，如“读取文件”或“打开网络连接”。每个角色都有一组相关的权限
- 会话（session）：会话由为执行特定任务而激活用户角色的子集组成。例如，笔记本电脑用户可以创建与管理员角色的会话，用来安装新程序
- 会话支持最小特权原则

基于角色的访问控制（Role-based Access Control）

分级RBAC

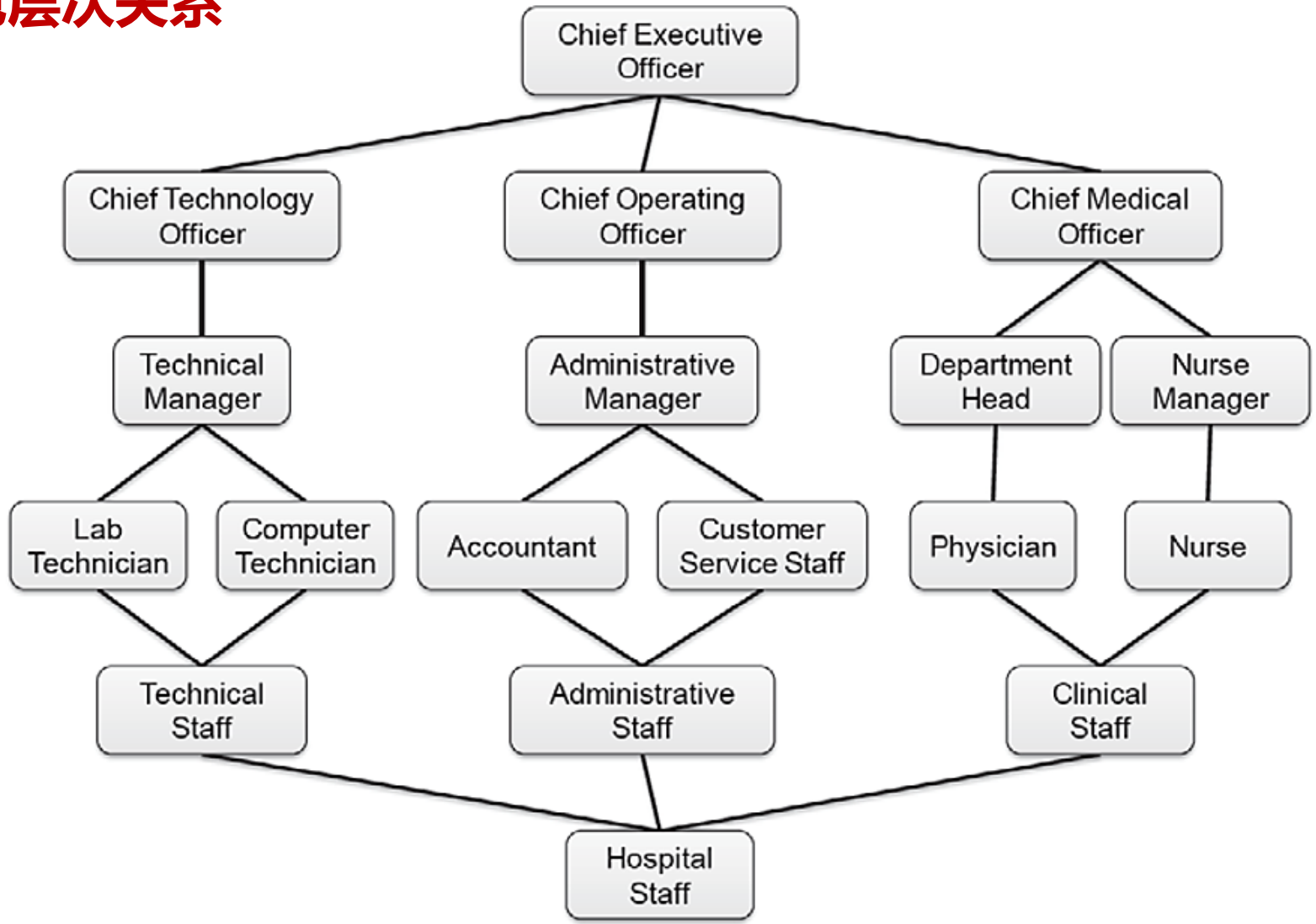
- 在基于角色的访问控制模型中，角色可以按照类似组织图的分层的层次结构进行结构。更加正式地说，将定义角色之间的偏序说为：角色R1**继承（inherits）**R2，如果R1包含R2的所有权限，R2包括R1的所有用户，可以表示为：

$$R1 \succcurlyeq R2$$

- 当R1 $\succcurlyeq$ R2时，我们也就说角色R1是R2的**上一层**（senior），或者R2是R1的**下一层**（junior）

基于角色的访问控制（Role-based Access Control）

可视化角色层次关系



提纲

PART 1 | 策略、模型与信任

PART 2 | 访问控制模型

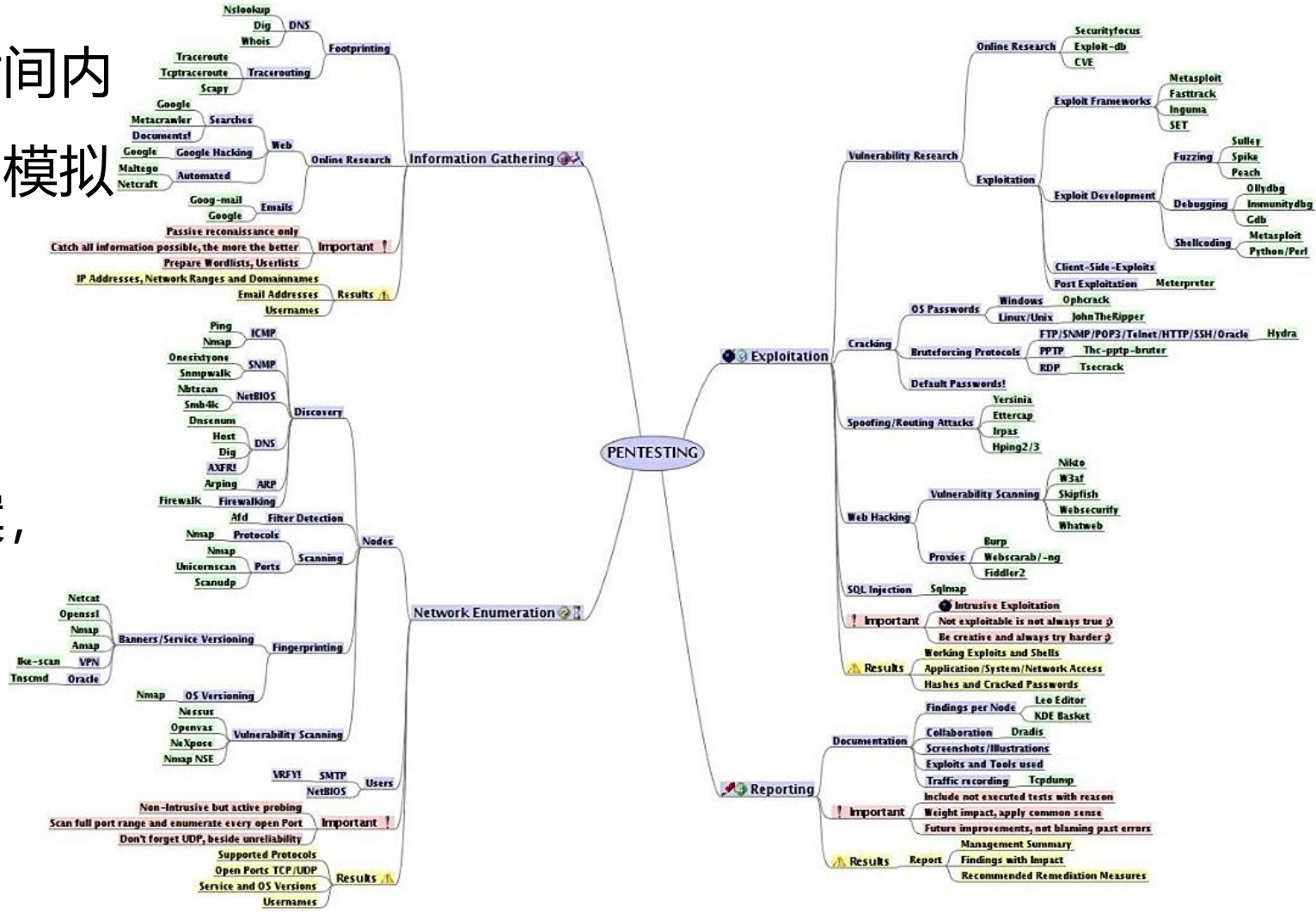
PART 3 | 渗透测试

PART 4 | Kerberos

PART 5 | 安全存储

渗透测试

- 从**攻击者**(黑客)的角度测试系统和体系结构的安全性，在固定时间内必须获得的具有预定目标的“模拟攻击”
- 渗透测试不是...
  - 其他IT安全措施的替代方案，它是对其他测试的补充
  - 安全保障
  - 获取漏洞的大花销的方法



渗透测试中的流程

- 收集信息（Gather Information）
- 扫描IP地址（Scan IP Addresses）
- 识别系统（Fingerprinting）
- 识别易受攻击服务（Identify Vulnerable Services）
- 利用漏洞（Exploit Vulnerability）

收集信息

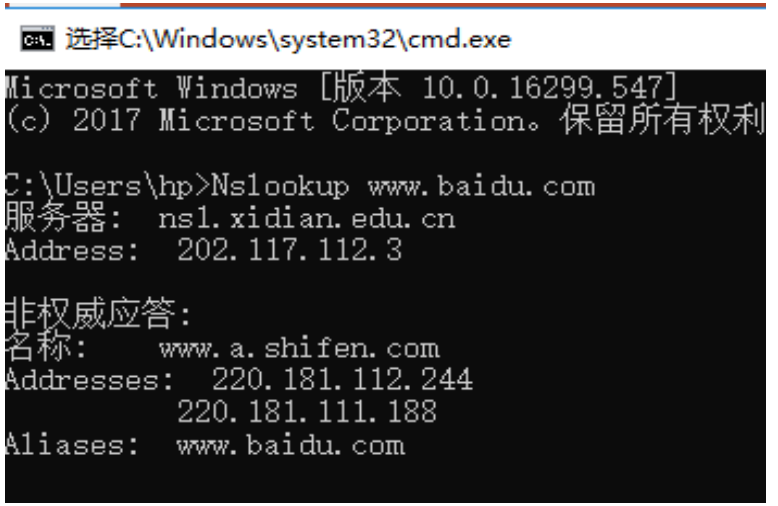
- 目标：给定一家公司的名称，确定以下信息

IP地址信息

- WHOIS ： 是用来查询域名的IP以及所有者等信息的传输协议。简单说，WHOIS就是一个用来查询域名是否已经被注册
- Nslookup：Nslookup可以指定查询的类型，可以查到DNS记录的生存时间还可以指定使用哪个DNS服务器进行解释。在已安装TCP/IP协议的电脑上面均可以使用这个命令

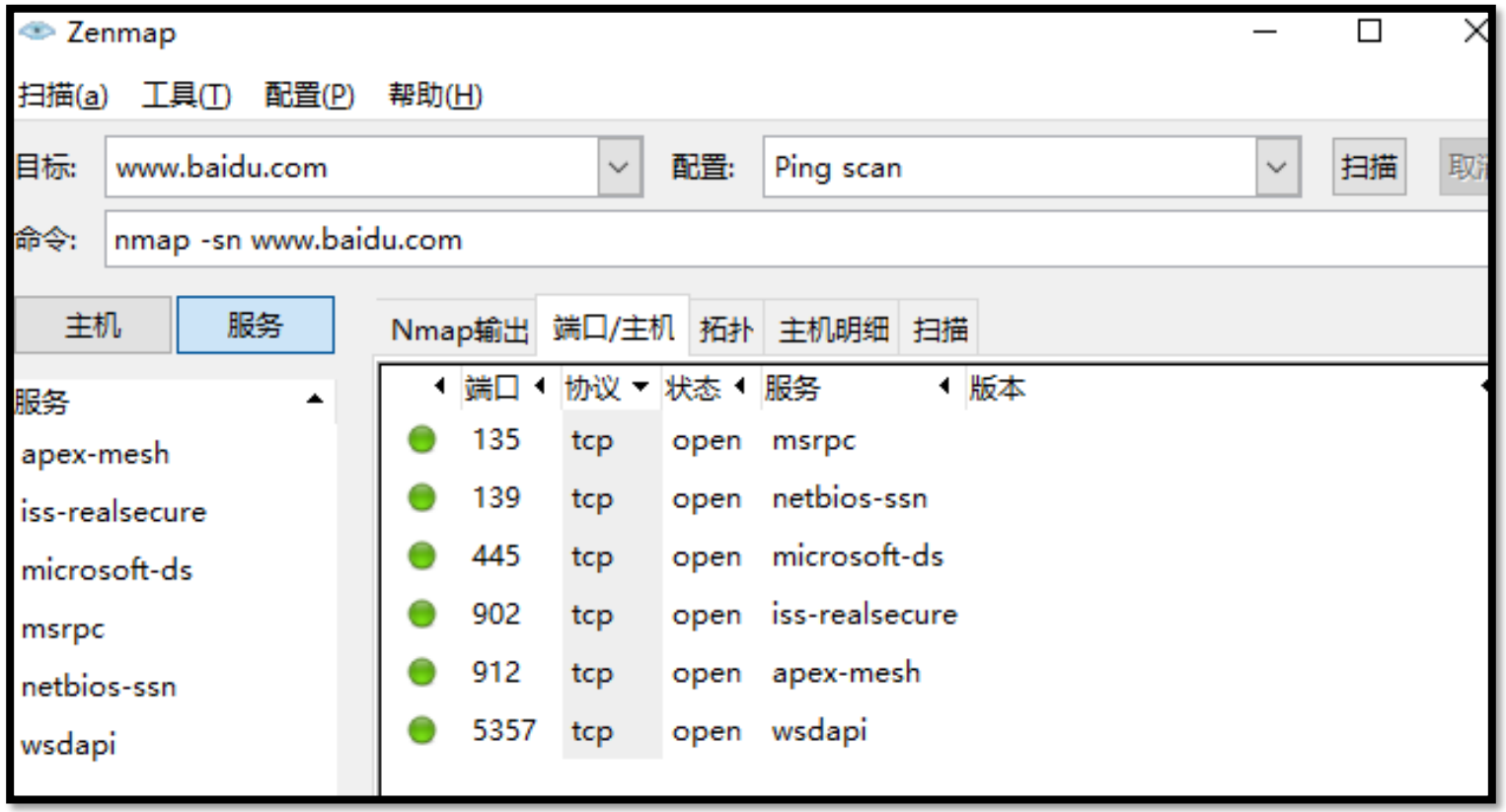
个人信息

- 在计算机科学中，社会工程学（social engineering）指的是通过与他人的合法地交流，来使其心理受到影响，做出某些动作或者是透露一些机密信息的方式。这通常被认为是一种欺诈他人以收集信息、行骗和入侵计算机系统的行为
- Google 或者 百度 等



扫描IP地址

- 目标：给定一组IP地址，确定每个服务和操作系统都在运行
- NMAP（Network Mapper）：是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端（https://nmap.org/）



扫描IP地址

NMAP常见命令

- Nmap的6种端口状态:
  - Open
  - Closed
  - Filtered: 可能被过滤，可能网络阻塞
  - Unfiltered: 可以访问，但未知端口处于开放还是关闭状态
  - Open|Filtered
  - Closed|Filtered:不能确定端口事关闭还说被过滤

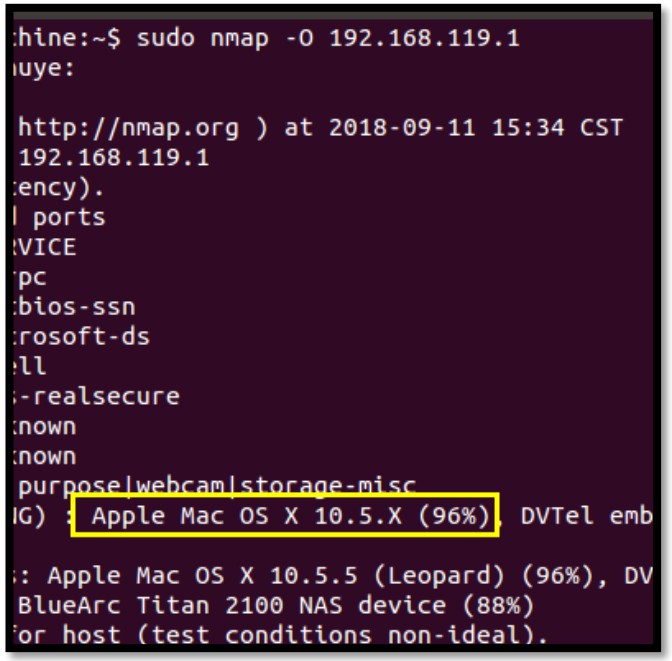
- 常见的扫描方式:
- 指定端口扫描:
  - nmap -p 80 172.20.62.150
- TCP SYN扫描：又称为半开放扫描，常见扫描方式，扫描速度较快，由于未进行TCP连接，比较隐蔽，很难被防火墙或管理员发现
  - nmap -sS 172.20.62.150(需要root权限)
- TCP ACK扫描：致命缺点是无法确定端口是否开放还是被过滤

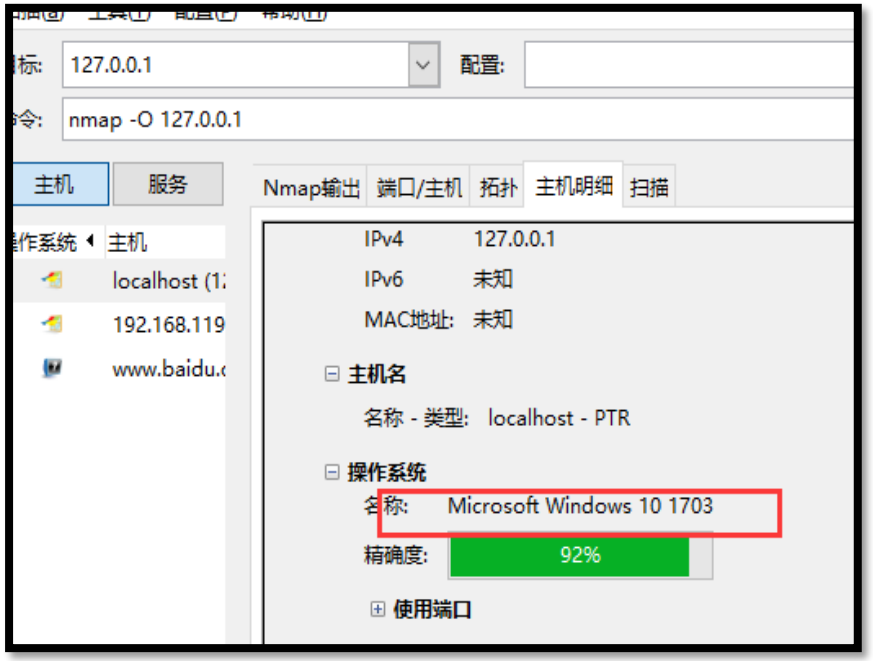
识别系统

- 通过扫描开放电脑的网络连接端，确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统（Fingerprinting）

- 主要任务
  - 哪个网络服务器在运行?
  - 找到了哪些帐户?
  - 哪些服务在运行?
  - 什么操作系统正在运行?
  - 谁登录了?
  - 网站上有可用的信息吗?

- 在NMAP中，使用命令nmap –O <目标IP地址>，即可得出目标主机的系统，如下图所示：





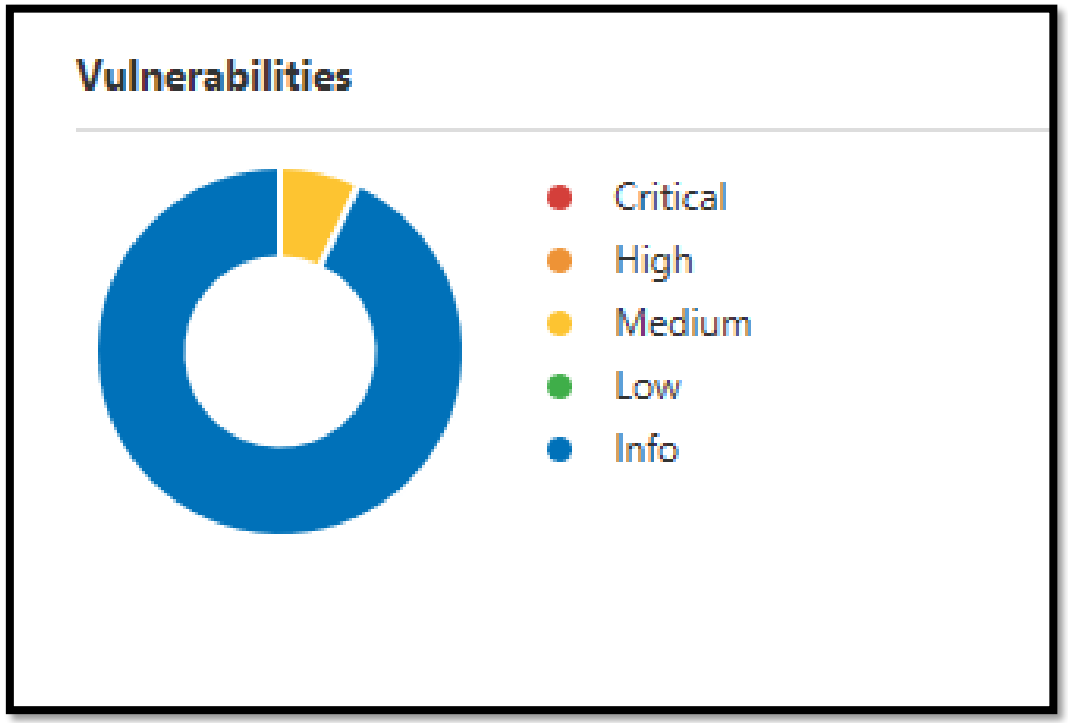
识别易受攻击服务

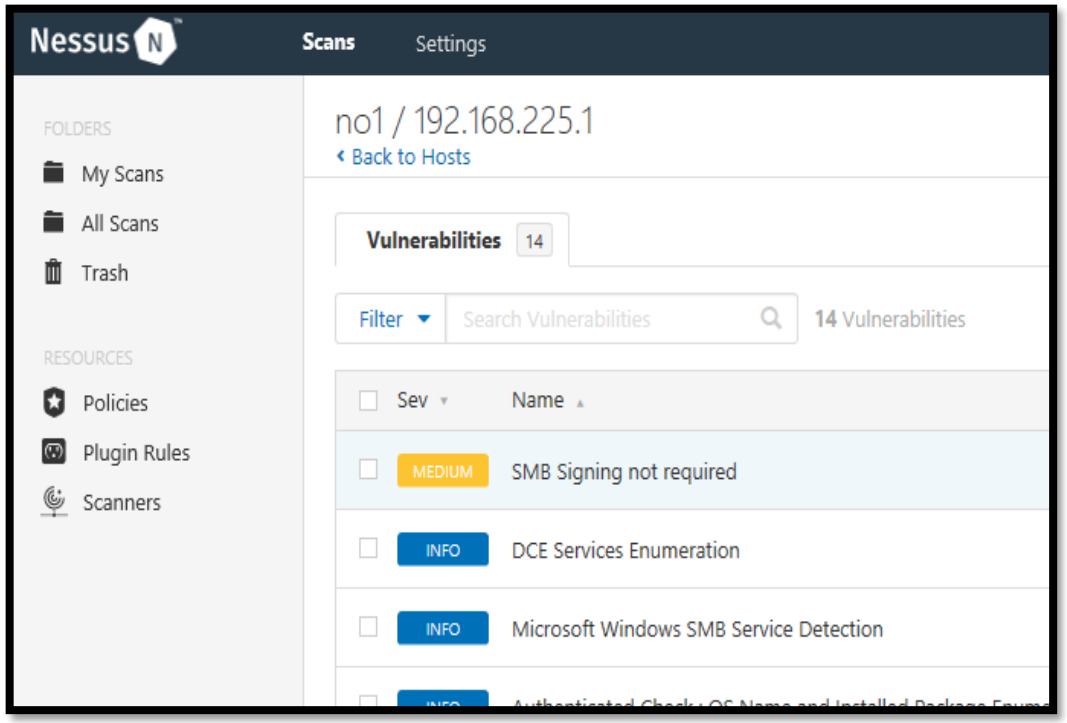
- 目标：给定特定的IP地址和端口，尝试获得对机器的访问权限，报告此目标的所有已知漏洞

- Nessus 是目前全世界最多人使用的系统漏洞扫描与分析软件。总共有超过75,000个机构使用Nessus作为扫描该机构电脑系统的软件
- 2002年时，Renaud（Nessus创始人） 与 Ron Gula，Jack Huffard 创办了一个名为 Tenable Network Security 的机构。在第三版的Nessus 发布之时，该机构收回了 Nessus 的版权与程序源代码 (原本为开放源代码)，并注册成为该机构的网站

识别易受攻击服务

- 下载安装好Nessus之后，便可以对目标网站进行漏洞扫描
- 下图是扫描漏洞的安全级别的分类，右图是对于目标网站（192.168.225.1 ）漏洞扫描的结果





利用漏洞

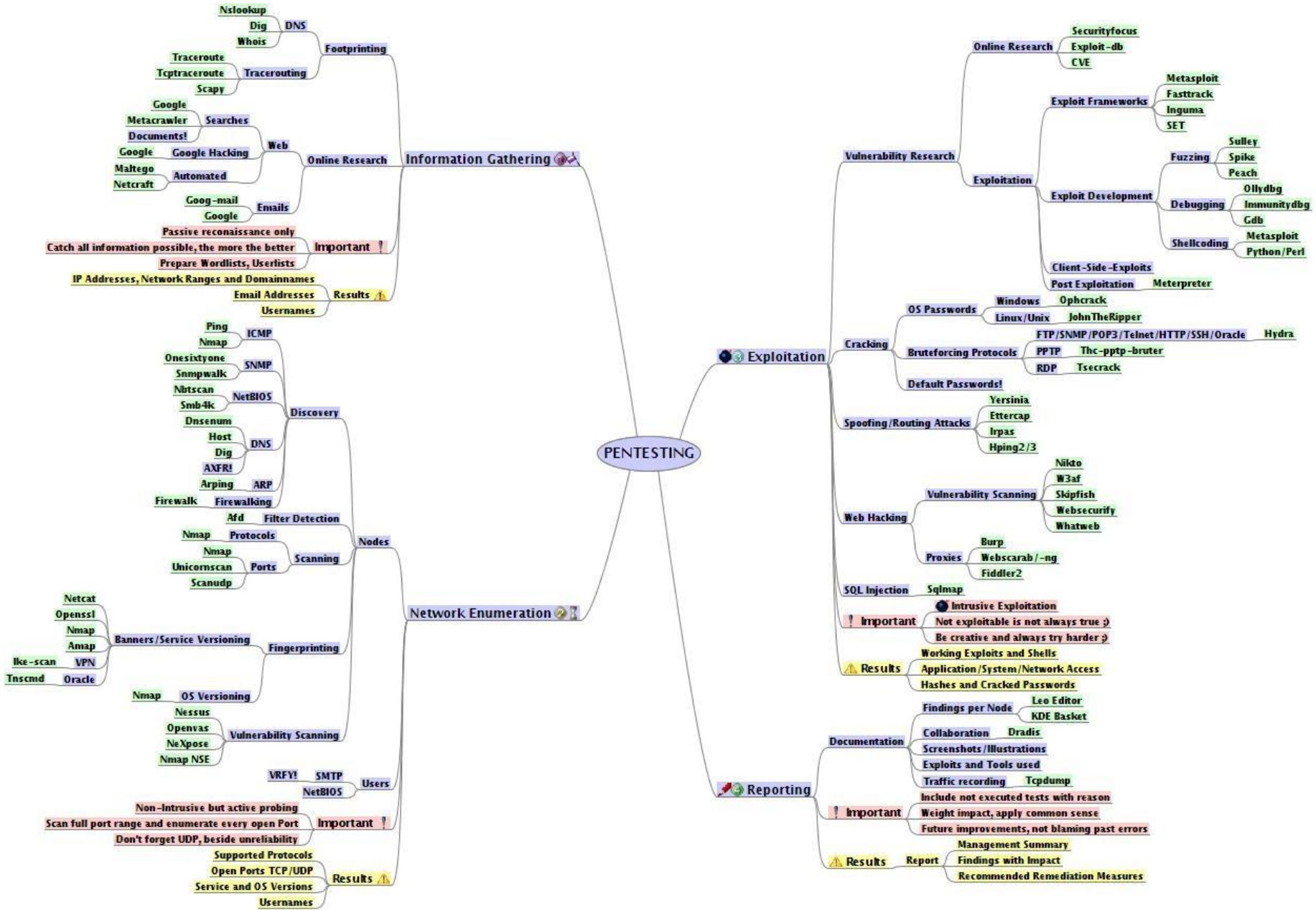
- 尝试利用检测到的漏洞，例如：
  - 缓冲区溢出（Buffer overflow）
  - 堆溢出（Heap overflow）
  - SQL注入（SQL injection）
  - 代码注入（Code injection）
  - 跨站脚本攻击（Cross-site scripting）

漏洞披露

- 如果我们发现一个新的漏洞（0day）...

- **Options**
  - 保守秘密，也许在将来，开发者会把发现并修好。
  - 告诉所有人或仅仅告诉开发者
    - 全面披露信息（太多）可能会帮助黑客爆破
    - 部分披露信息（太少）并没什么用
  - 卖掉，许多互联网公司，如微软、Facebook、Google，苹果等都有一种悬赏机制，只要黑客发现他们产品存在的漏洞并报告给他们，这些公司就会向这些黑客提供奖金

渗透测试


PENTESTING
Information Gathering
Footprinting
DNS
Nslookup
Dig
Whois
Tracerouting
Traceroute
Tcptraceroute
Scapy
Online Research
Web
Searches
Google
Metacrawler
Documents!
Google Hacking
Google
Automated
Maltego
Netcraft
Emails
Goog-mail
Google
Important
Passive reconaissance only
Catch all information possible, the more the better
Prepare Wordlists, Userlists
Results
IP Addresses, Network Ranges and Domainnames
Email Addresses
Usernames
Network Enumeration
Nodes
Discovery
ICMP
Ping
Nmap
SNMP
Onesixtyone
Snmpwalk
NetBIOS
Nbtscan
Smb4k
DNS
Dnsenum
Host
Dig
AXFR!
ARP
Arping
Firewalking
Firewalk
Filter Detection
Afd
Scanning
Protocols
Nmap
Ports
Nmap
Unicornscan
Scanudp
Fingerprinting
Banners/Service Versioning
Netcat
Openssl
Nmap
Amap
VPN
Ike-scan
Oracle
Tnscmd
OS Versioning
Nmap
Vulnerability Scanning
Nessus
Openvas
NeXpose
Nmap NSE
Users
SMTP
VRFY!
NetBIOS
Important
Non-Intrusive but active probing
Scan full port range and enumerate every open Port
Don't forget UDP, beside unreliability
Results
Supported Protocols
Open Ports TCP/UDP
Service and OS Versions
Usernames
Exploitation
Vulnerability Research
Online Research
Securityfocus
Exploit-db
CVE
Exploitation
Exploit Frameworks
Metasploit
Fasttrack
Inguma
SET
Exploit Development
Fuzzing
Sulley
Spike
Peach
Debugging
Ollydbg
Immunitydbg
Gdb
Shellcoding
Metasploit
Python/Perl
Client-Side-Exploits
Post Exploitation
Meterpreter
Cracking
OS Passwords
Windows
Ophcrack
Linux/Unix
JohnTheRipper
Bruteforcing Protocols
FTP/SNMP/POP3/Telnet/HTTP/SSH/Oracle
Hydra
PPTP
Thc-pptp-bruter
RDP
Tsecrack
Default Passwords!
Spoofing/Routing Attacks
Yersinia
Ettercap
Irpas
Hping2/3
Web Hacking
Vulnerability Scanning
Nikto
W3af
Skipfish
Websecurify
Whatweb
Proxies
Burp
Webscarab/-ng
Fiddler2
SQL Injection
Sqlmap
Important
Intrusive Exploitation
Not exploitable is not always true ;)
Be creative and always try harder ;)
Results
Working Exploits and Shells
Application/System/Network Access
Hashes and Cracked Passwords
Reporting
Documentation
Findings per Node
Leo Editor
KDE Basket
Collaboration
Dradis
Screenshots/Illustrations
Exploits and Tools used
Traffic recording
Tcpdump
Important
Include not executed tests with reason
Weight impact, apply common sense
Future improvements, not blaming past errors
Results
Report
Management Summary
Findings with Impact
Recommended Remediation Measures

提纲

PART 1 | 策略、模型与信任

PART 2 | 访问控制模型

PART 3 | 渗透测试

PART 4 | Kerberos

PART 5 | 安全存储

Kerberos

- Kerberos：基于**可信第三方（Trusted Third Party，TTP）**的认证协议
- MIT的雅典娜项目组（Athena Group）开发的认证服务系统
- 使用Kerberos身份验证的服务通常被称为“**Kerberized**”
- Kerberos使用票据（ticket）的概念作为证明用户身份令牌
- 票据是存储会话密钥的数字文件。在登录会话中，通常会发送会话密钥，然后代替在kerberized服务中的密码

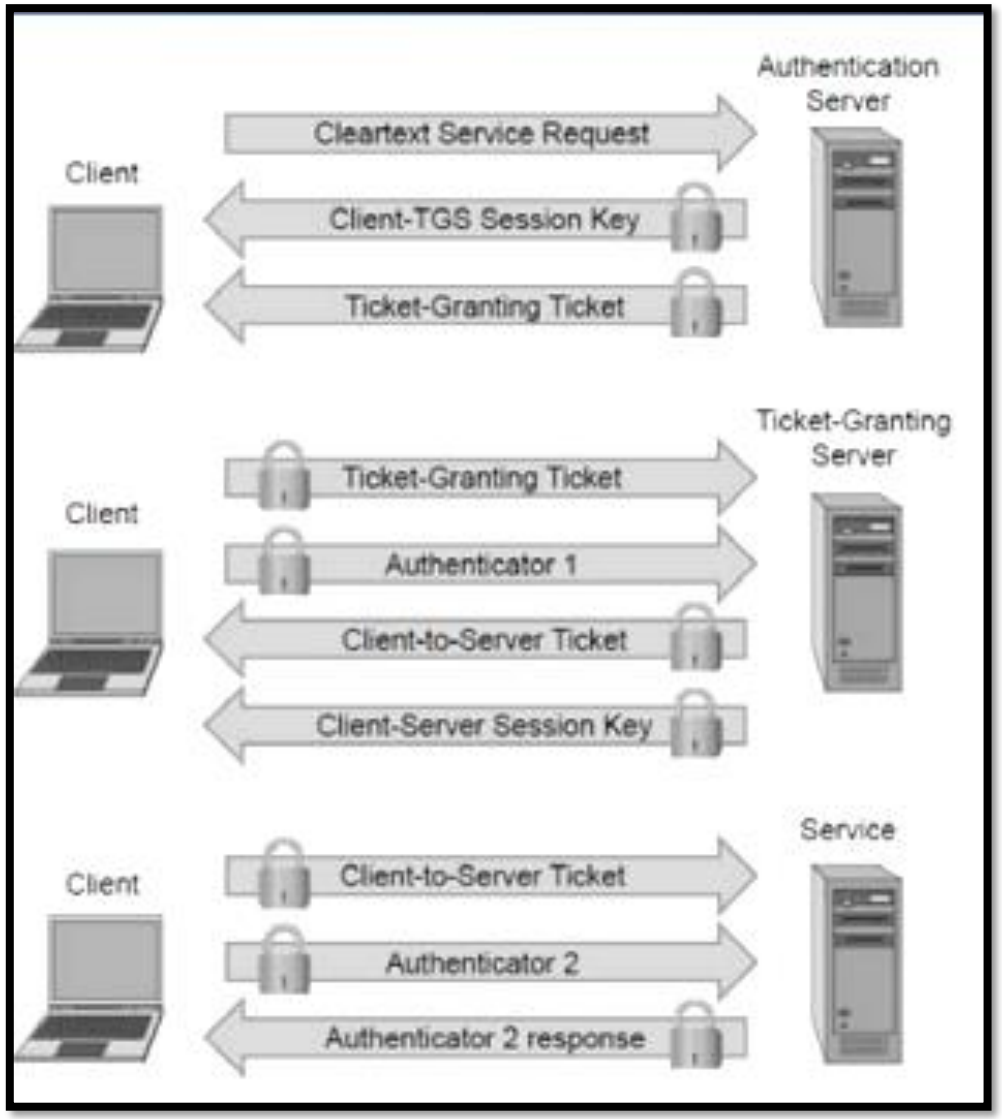
Kerberos是希腊神话中地狱看门的三头犬的名字

Kerberos

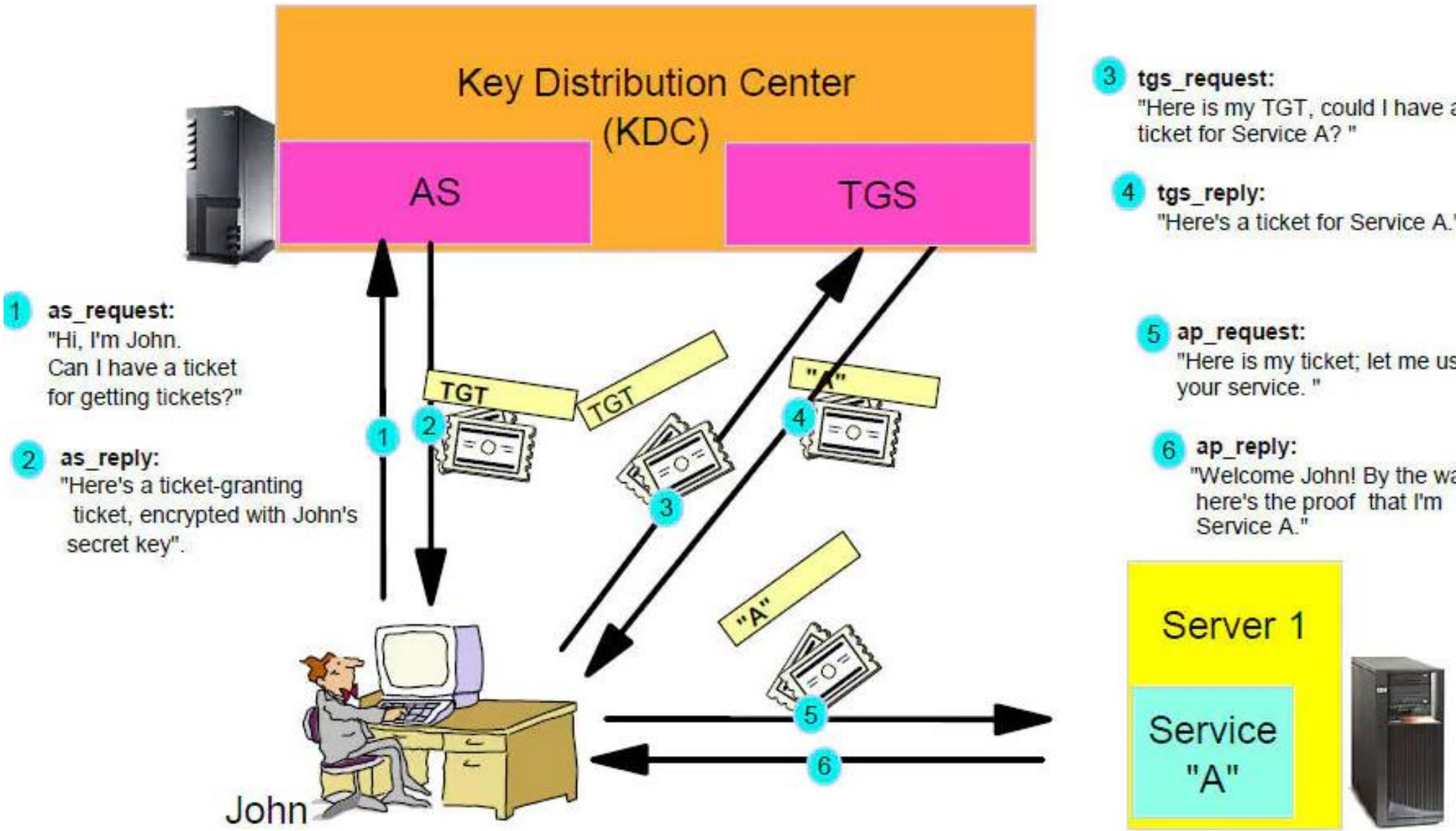
- 在身份验证过程中，客户端会收到**两个票据**
  - 票据授予票据（ticket-granting ticket，TGT）：用户和会话密钥的全局标识符
  - 服务票据（service ticket）：对用户进行身份验证，确定用户能否使用特殊服务
- 这些票据都有时间戳，用于表明票据的有效期限，Kerberos管理员可以根据票据服务来设置其到期时间
- 为了实现安全的身份验证，Kerberos使用可信第三方作为**密钥分发中心**（key distribution center，KDC），由**两个部分**组成
  - 身份验证服务器（authentication server，AS）：用于执行用户身份验证
  - 票据授予服务器（ticket granting server，TGS）：用于向用户授予票据
- 身份验证服务器维护存储用户和服务密钥的数据库，对用户提供的密码执行单向散列来生成用户的密钥

Kerberos身份认证

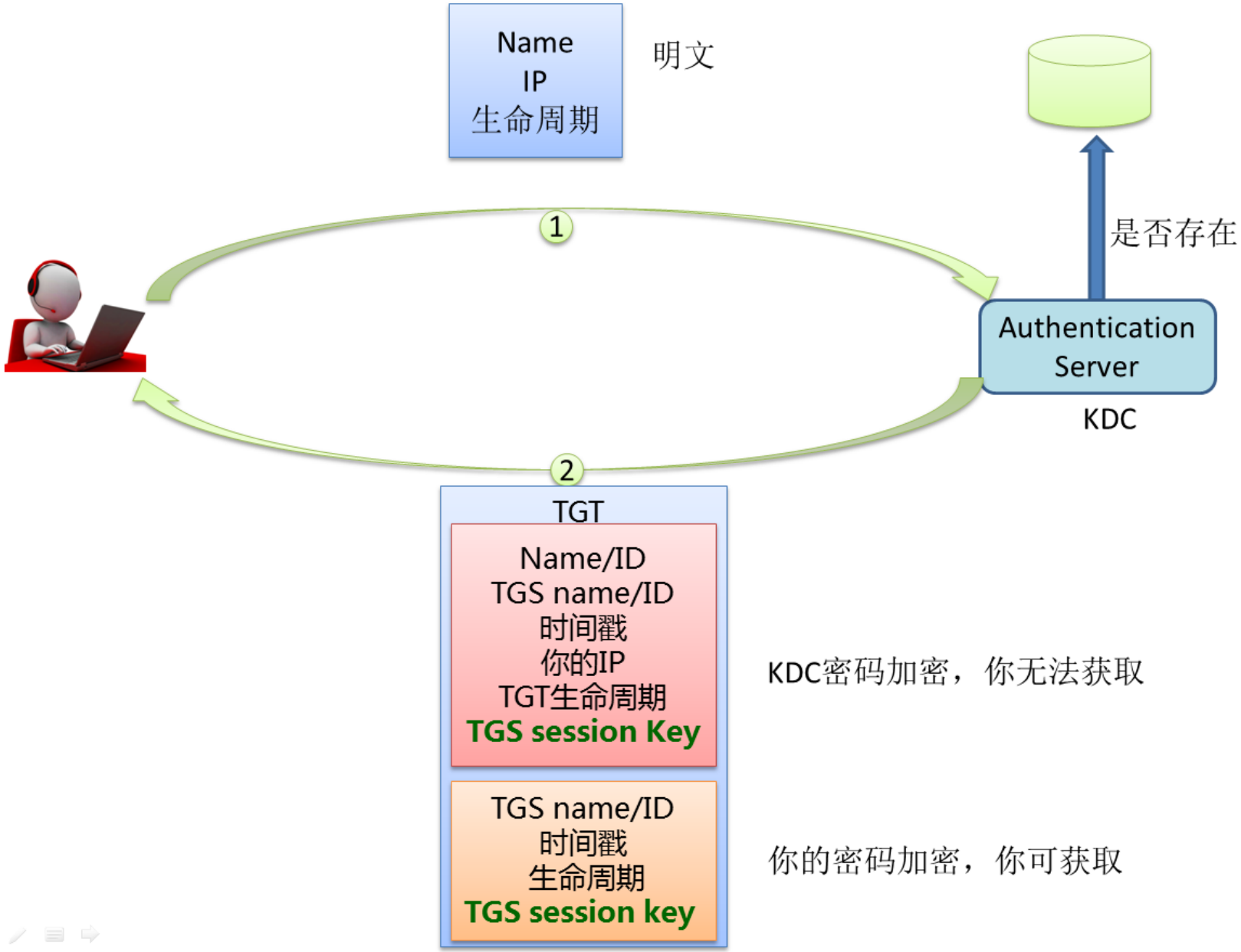
- 客户端与身份验证服务器（AS）互相进行身份验证
- 客户端与票据授予服务（TGS）互相进行身份验证
- 客户端与服务（S）互相进行身份验证，此要为客户端提供服务



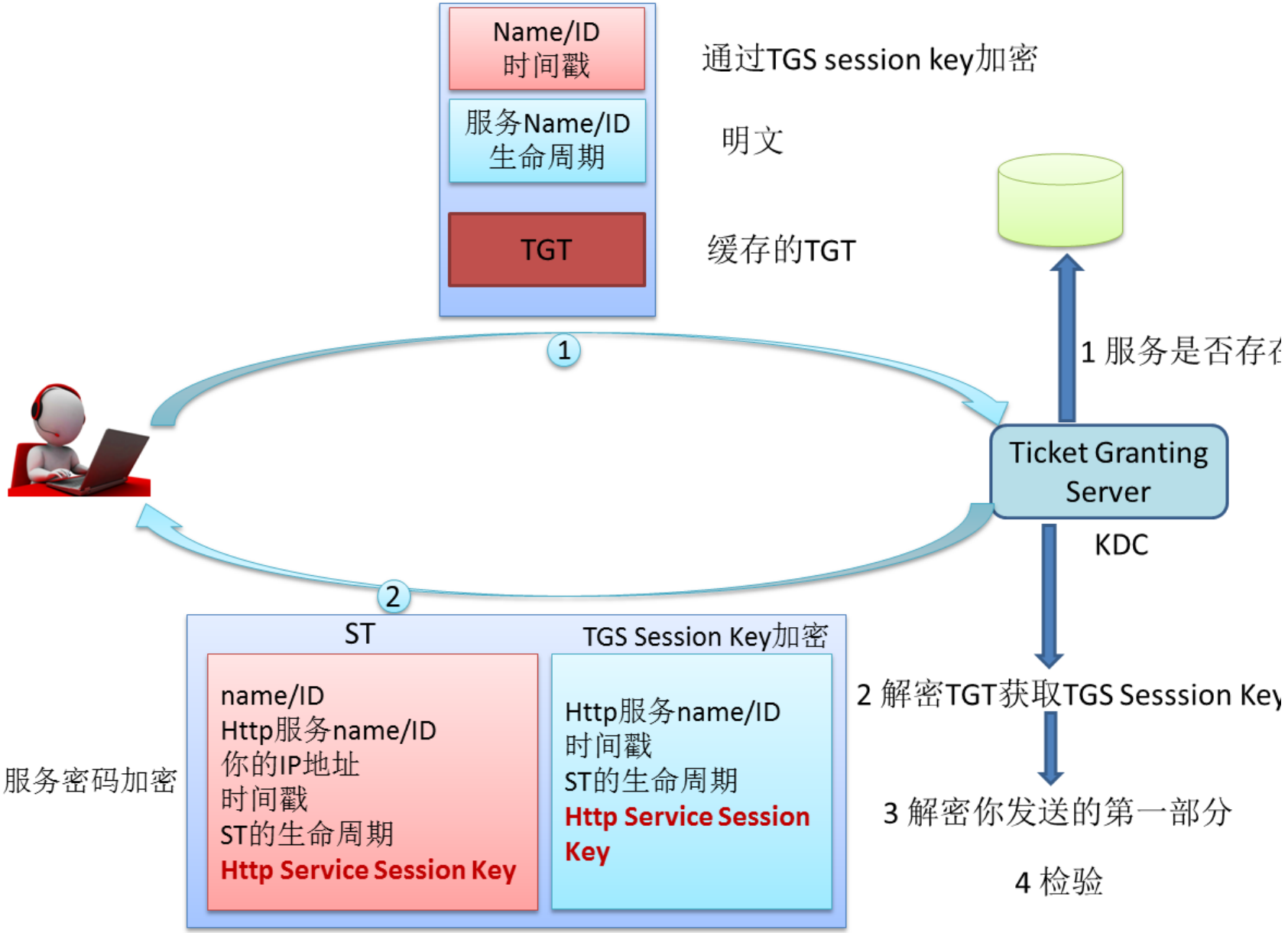
Kerberos身份认证



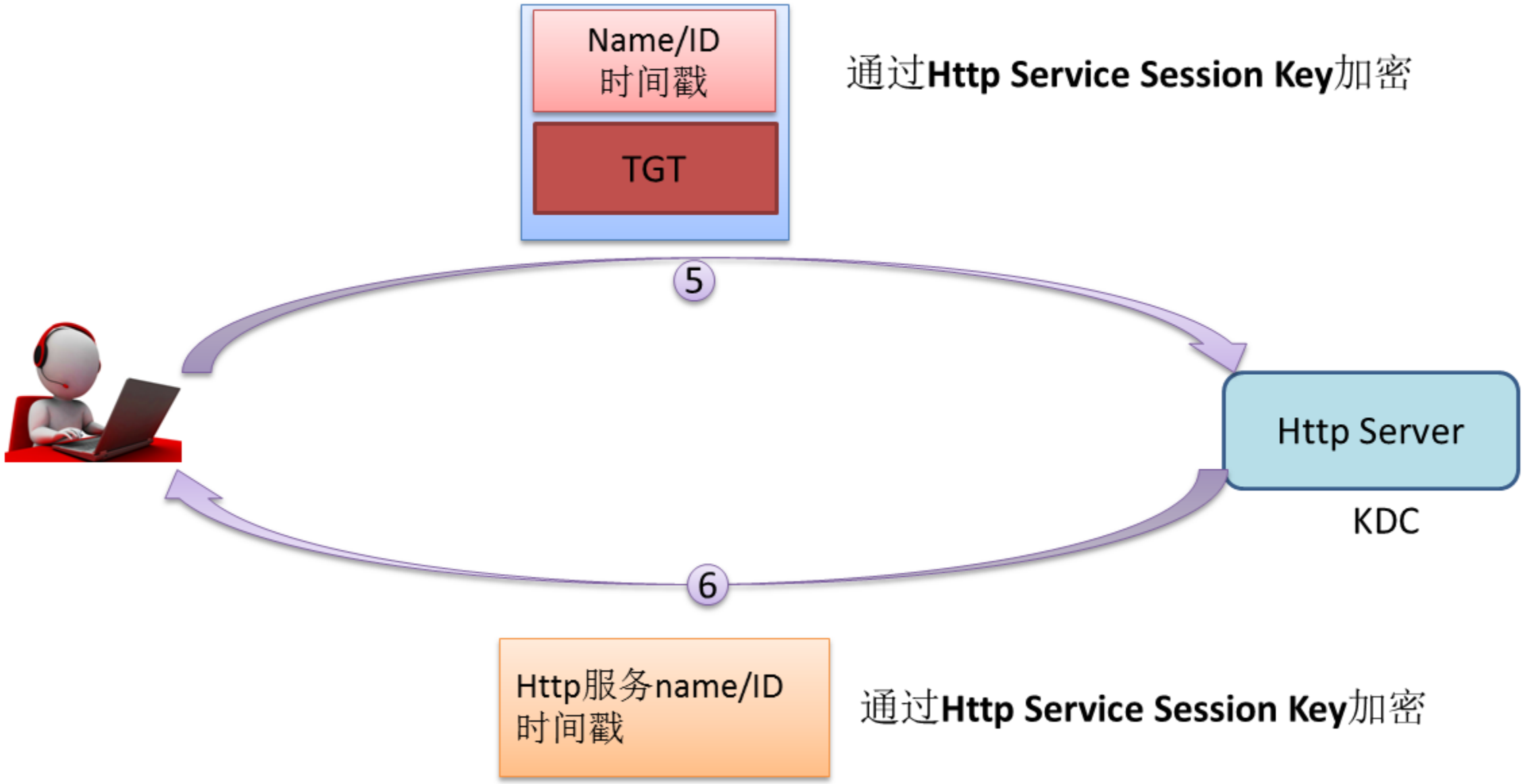
Kerberos身份认证-第一阶段



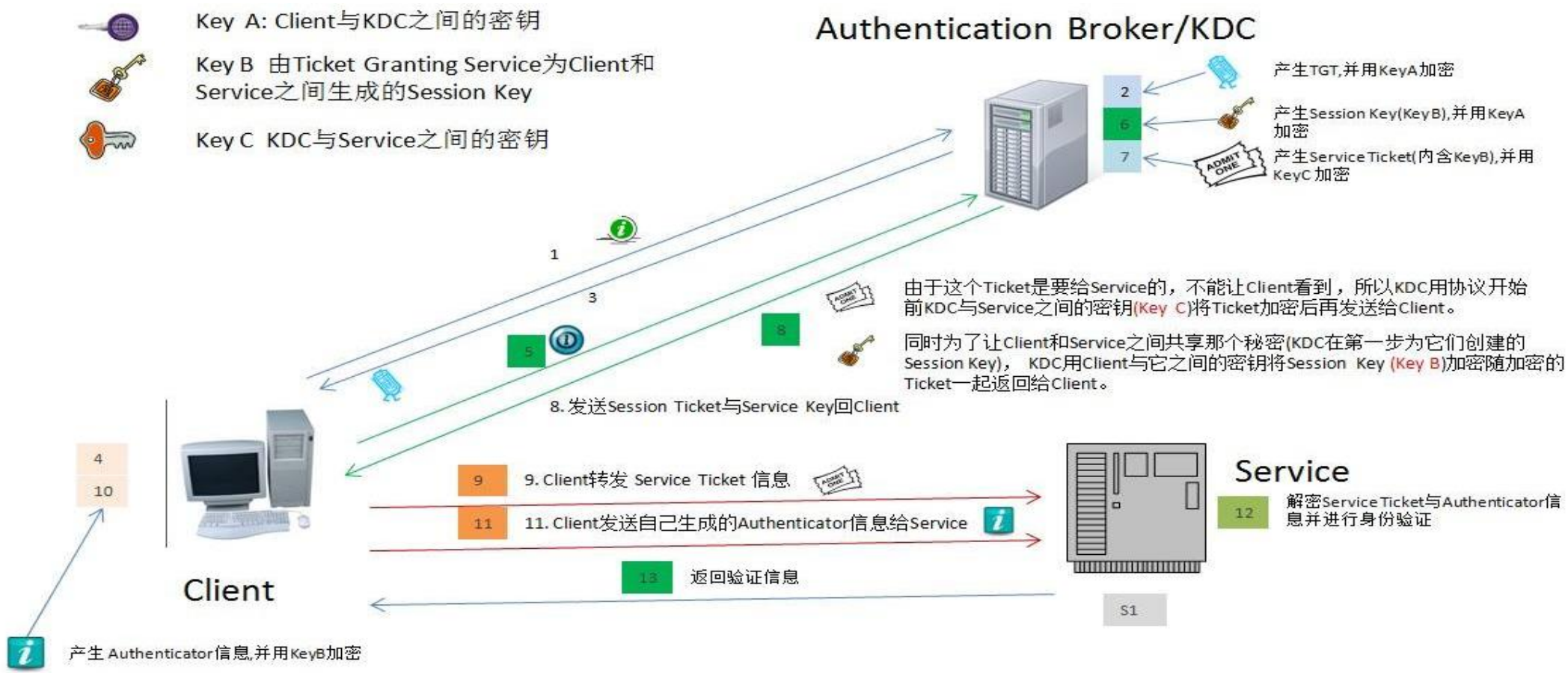
Kerberos身份认证-第二阶段



Kerberos身份认证-第三阶段



Kerberos身份认证



Info C: Client自己的身份信息

Info CS:Client发给KDC的所要请求的服务信息(服务名等)

Info Authen: Client将收到的Session Key解密出来，然后将自己的用户名，用户地址（IP）打包成Authenticator

TGT: ticket-granting ticket， 由 Ticket Granting Service授予

Service Tictket:此Ticket是要给Service的， 不能让Client看到，所以生成后要用KeyC加密

Kerberos的优点

- 由于Kerberos协议的分布式体系结构，甚至在不安全的网络使用Kerberos协议也是安全的
- 由于每次传输都使用适当的密钥进行加密，攻击者在不能破解密钥或底层的加密算法的情况下，无法伪造有效的票据来获得对未授权服务的访问
- 当攻击者窃听合法的Kerberos通信，从未授权方重传消息来执行未授权操作时，Kerberos的设计还能防止重放攻击
- Kerberos使用的是对称加密，而不是公钥加密，这使得Kerberos的计算效率更加高效

Kerberos的缺点

- Kerberos存在单点故障
  - 如果密钥分发中心不可用，则整个网络的身份验证方案可能停止工作
    - 大型网络有时使有多个KDC，或在紧急情况下有备用KDC可用，以来防止这种情况
- 如果攻击者破坏了KDC，网络上每个客户端和服务器的身份验证信息都会被泄露
- Kerberos因为使用了时间戳，要求所有参与方都有同步时钟

提纲

PART 1 | 策略、模型与信任

PART 2 | 访问控制模型

PART 3 | 渗透测试

PART 4 | Kerberos

PART 5 | 安全存储

安全存储

- 在美国机场每周大约有12000台笔记本丢失或被盗，除了更换设备的费用之外，丢失笔记本电脑也会产生数据泄露的风险
- 研究表明，丢失笔记本的平均费用大约是5万美元，这不仅仅是硬件的损失，而主要是知识产权的损失，取证的相关费用，生产力的损失及法律费用
- 为了缓解这一问题，已经研究了一些技术用于保护计算机系统中数据的机密性，甚至在物理入侵中，这些技术也能有效的保护数据的机密性

安全事件

- 2016年9月，雅虎公司曾宣布，黑客2013年8月盗走其至少5亿用户的账户信息。当年12月，雅虎又表示，被盗账户数量约10亿个。据2017年10月3日发布的信息，雅虎公司证实，其所有30亿个用户账号应该都受到了黑客攻击的影响，公司已经向更多用户发送提示，请其更改登录密码以及相关登录信息

- 2018年8月28日，华住集团旗下连锁酒店疑似发生用户数据泄露。在暗网中，一位ID名为“helen250”的用户发帖出售华住旗下酒店入住用户数据包，这些数据涉及1.3亿条身份信息、2.4亿条开房记录等共5亿条信息，被标价为8比特币或520门罗币，约37万人民币出售，涉及的酒店包括汉庭、美爵、禧玥、诺富特等

安全保护措施

- 拿好USB驱动器和智能手机，谨防丢失
- 防范窃取数据的恶意软件
- 防范设备被扣押
- 合理回收过时或有故障的设备，谨防丢失
- 在其他设备上备份
- 云存储

文件密码保护

- 保护信息的一种方法就是**对文件进行加密**，在密码算法没有在理论破解或密钥泄露的情况下，即使文件被盗，也不用担心信息会泄露
- 文件加密旨在有效的防御确定的攻击者。如Office中可供使用的加密算法取决于Windows 操作系统中可通过 API访问的算法；除了可以保持对加密API (CryptoAPI) 的支持之外， Office2016也支持CNG （CryptoAPI Next Generation），可指定主计算机上支持的加密和哈希算法，以供文档加密使用
  - 以下 CNG 加密算法和哈希算法或安装在系统上的任何其他 CNG 加密扩展均可用于 2007 Office system SP2、Office 2010、Office 2013 或 Office 2016

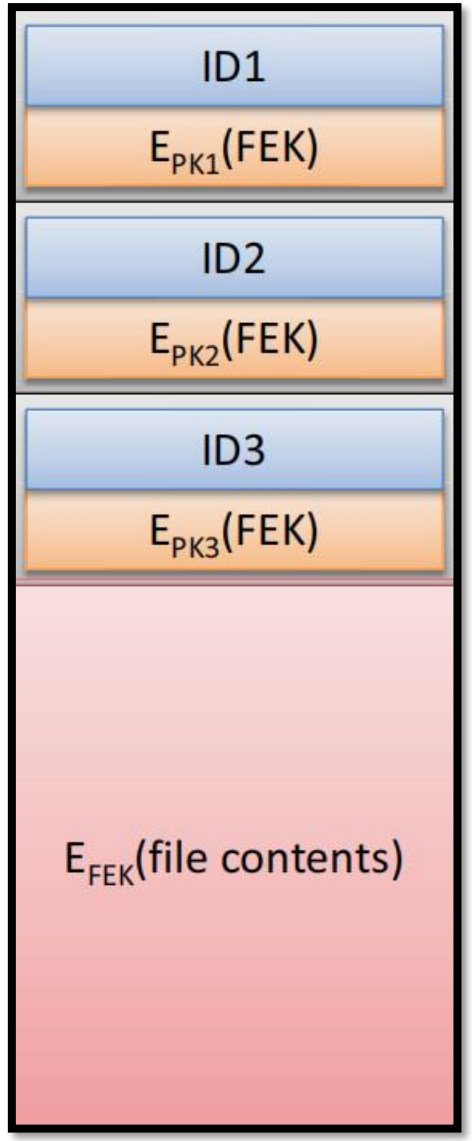
- 加密算法：AES、DES、DESX、3DES、3DES_112 和 RC2
- 哈希算法：MD2、MD4、MD5、RIPEMD-128、RIPEMD-160、SHA-1、SHA256、SHA384 和 SHA512

加密文件系统（EFS）

- 加密文件系统（Encrypting File System，EFS）是文件系统级加密方案的一个示例，Windows 2000以后的系统皆可用
- 特点
  - EFS的工作原理是透明的，能自动对指定文件和文件夹进行加密和解密
  - 保护文件内容，但不保护文件名和其他元数据
  - 支持共享加密文件
  - 最新版本使用RSA、IDEA、AES和SHA-256
- 缺点
  - 只保护本地文件系统，所以将文件传送到其他文件系统会导致意外的破解
  - 文件内容可能泄露给不受保护的临时文件
  - 密钥管理很麻烦

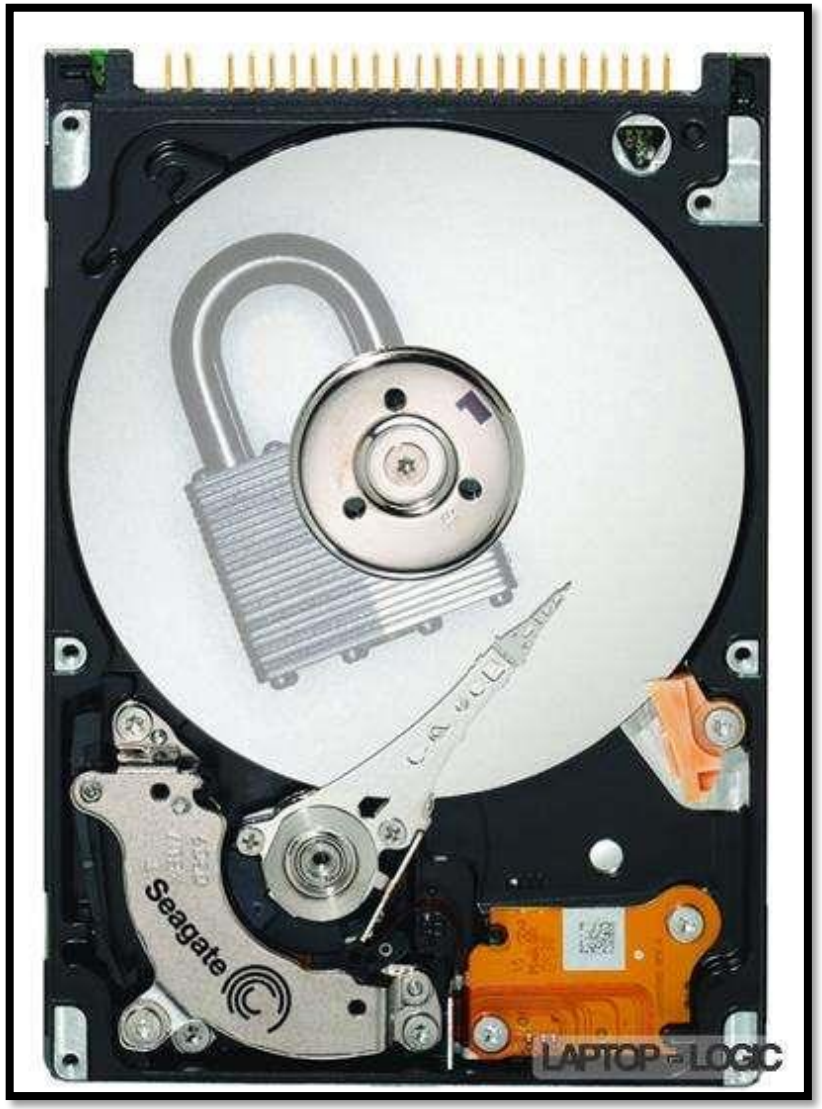
加密文件系统（EFS）

- EFS使用对称和非对称加密技术，首先使用（对称加密算法）AES单独的对称加密密钥（file-encryption key，FEK）加密每个文件，然后使用FEK加密数据，再用用户的（非对称加密算法）RSA的公钥加密FEK，并保存文件的元数据
- 为了解密文件，先用用户的私钥解密FEK，然后再用FEK解密数据，为了支持用户之间的共享，在加密文件中可以包含多个FEK副本，每个副本用不同的用户公钥加密，如图所示，每个用户对应有一个经过公钥加密过的FEK



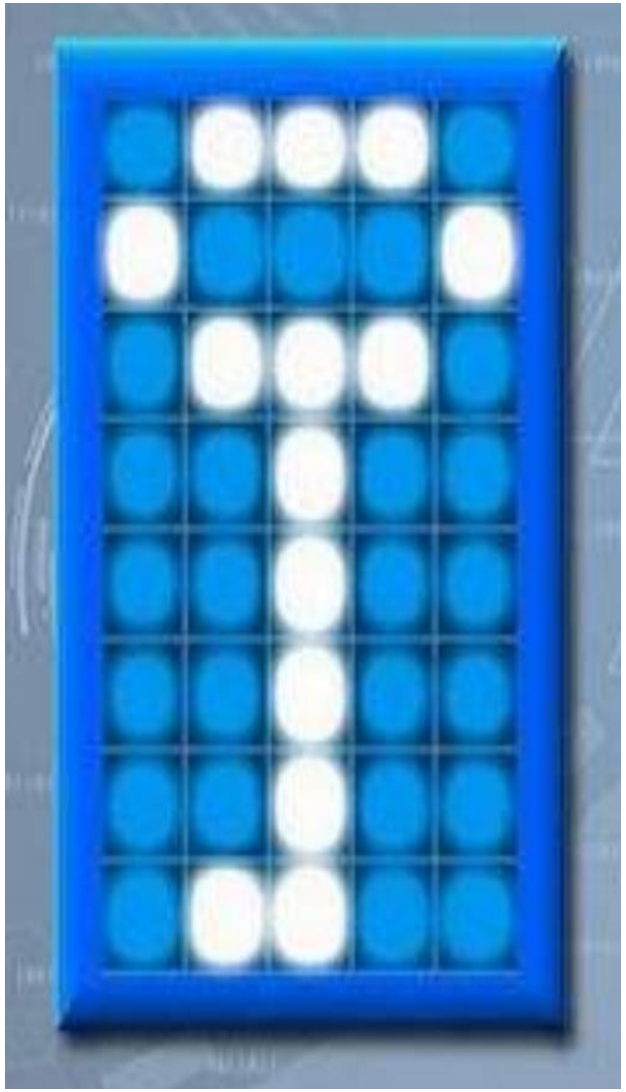
磁盘加密

- TrueCrypt是一款免费开源的加密软件，同时支持Windows Vista，7/XP，Mac OS X，Linux 等操作系统
- BitLocker驱动器加密是在Windows Vista中新增的一种数据保护功能，主要用于解决一个人们越来越关心的问题：由计算机设备的物理丢失导致的数据失窃或恶意泄漏，在Windows 8.1中也能使用此加密驱动



磁盘加密——TrueCrypt

- 所有加密都是以分区为基础的
- 真加密，所有加密数据都是经过AES等加密算法的运算后的结果，无法破解（穷举法除外）
- 能创建加密的“虚拟磁盘文件”
- 加密单个分区或整个硬盘
- 加密Windows系统所在的分区（启动Windows前需要密码）
- 加密过程自动、实时、透明（使用加密文件或分区前输入密码，载入后就可以像使用一个普通分区一样使用加密分区）

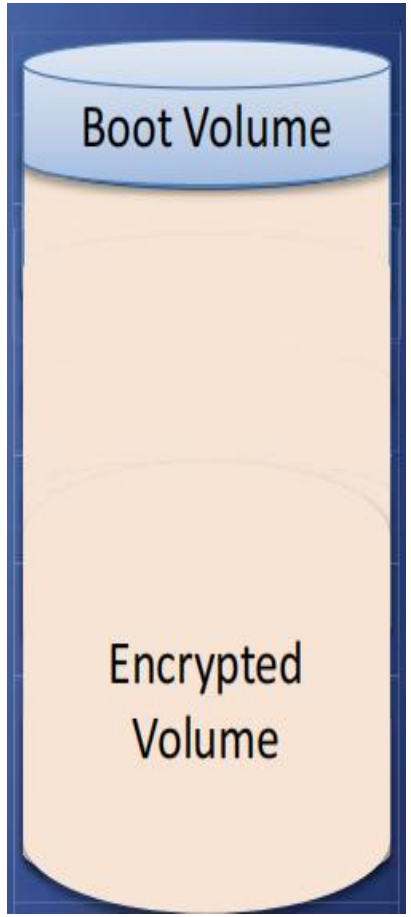


磁盘加密——TrueCrypt

- 提供两级方案，以应对被强迫说出密码的情况，如（抢劫等）
  - 隐藏分区（覆盖式密码术，steganography）、隐藏操作系统
  - 无法探测到 TrueCrypt 加密分区（加密数据会被认为是随机数据）
- 加密算法：AES-256、Serpent、Twofish。为取得更好加密效果，可以同时使用两种或三种加密算法。
- **Remark**：2014年5月28日，TrueCrypt将其网站转址回SourceForge，并在其页面警告该软件可能包含未修复的安全性问题，且TrueCrypt的开发已在2014年5月微软终止Windows XP支持后结束。该站亦提供一个新版的TrueCrypt（7.2）下载，此版本仅有解密功能

磁盘加密——BitLocker

- BitLocker使用对称加密（AES）对磁盘扇区进行加密。为了解密卷，用户可以在引导时通过键盘输入密码，或从USB驱动器或可信平台模块（Trusted Platform Module，TPM）加载解密密钥
- BitLocker使用两个NTFS格式的卷（Volume），一个卷包含操作系统和加密的数据（Encrypted Volume），另一个卷作为未加密的引导卷（Boot Volume）。当在引导时对用户进行身份验证，则解锁卷的主密钥（Volume Master Key）。使用主密钥，BitLocker解密全卷的加密密钥（Full-Volume Encryption Key，FVMK），FVMK被加密后存储于引导卷中，然后全卷的加密密钥存储在内存中，用于解密加密卷中的数据



磁盘加密——BitLocker

对BitLocker的攻击

- 使用TPM存储卷的主密钥增加了BitLocker的可以性，因为用户不用再输入密码或插入USB令牌，但是，BitLocker在这种操作模式下容易遭到冷启动攻击
- **冷启动(Cold Boot)攻击**属于一种边信道攻击方法，可以物理接触到计算机的攻击者能够运用这种攻击手段在冷启动或硬盘重启之后，比如计算机没经历正常的关机过程就突然重启时，从计算机的内存(RAM)中获取加密密钥、口令和其他数据。断电后内存中的数据能维持几十秒或数分钟，但通过液氮或压缩空气冷冻，这一数据衰减过程可被攻击者拉长至数小时之久

可信平台模块（Trusted Platform Module）

- **可信平台模块（TPM）**是设计安装在主板上的芯片，作为安全密码处理器，它能安全地生成和存储密钥。在生产时，将一个唯一地RSA私钥铸入到每一个TPM芯片中。TPM的设计是防篡改的，所以，能进行物理访问的攻击者也很难恢复这个密钥

- TPM芯片有一些**平台配置寄存器**（platform configuration registers，PCRs），用于存储一些加密操作的密钥和密文
  - extend操作：用PCR前一个值的加密散列更新指定的PCR，该PCR与为操作提供的数据相关联
  - seal操作：使用TPM私钥加密所提供的明文，并将它与当前指定的PCR内容相关联。这个操作返回密文，并根据指定的PCR和TPM私钥的当前值计算MAC
  - unseal操作：给定密文、散列值和PCR名称，如果计算出的当前PCR值得MAC与给定的散列值相同，则unseal操作会对铭文解密

可信平台模块（Trusted Platform Module）

对TPM的攻击

- 2010年安全研究人员Christopher Tarnovsky发现TPM芯片（英飞凌的SLE66CLPE）存在一个安全漏洞并且在2010年黑帽会议上展示了他的攻击效果。他表示，破解这种芯片是一个很漫长的过程，还要使用一台电子显微镜(零售价大约7万美元)。这个芯片破解的计划和实施用了6个月的时间，包括使用酸性溶液溶解这个芯片的外壳和使用微小的探针窃听芯片的编程指令
- 虽然攻击能够实现，但是Tarnovsky的做法技术操作性很强，而且需要将近半年的耐心工作，花费的代价太大。目前还不具备成熟的攻击技术

作业

- R-9.1
- R-9.3
- C-9.5

扩展补充

《网络安全法》

中国与网络安全的相关法律法规

犯罪 – 刑事处罚：《刑　法》

违法 – 治安处罚：《治安管理处罚法》

处分 – 从业禁止：《网 络 安 全 法》

后果很严重

《刑法》第285、286条主要罪名

后果很严重

《刑法》第二百八十五条

【非法侵入计算机信息系统罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

【非法获取计算机信息系统数据、非法控制计算机信息系统罪】违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

【提供侵入、非法控制计算机信息系统的程序、工具罪】提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

违反国家规定侵入

国家事务

国防建设

尖端科学技术领域

三年以下有期徒刑或者拘役

非法获取计算机信息系统数据、非法控制计算机信息系统罪

违反国家规定进行以下行为

侵入前款规定以外的计算机信息**系统**

采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的**数据**

对该计算机信息系统实施**非法控制**

情节严重: 三年以下有期徒刑或者拘役，并处或者单处罚金

情节特别严重: 三年以上七年以下有期徒刑，并处罚金

情节严重

（一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；

（二）获取第（一）项以外的身份认证信息五百组以上的；

（三）非法控制计算机信息系统二十台以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）其他情节严重的情形。

情节特别严重

（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；（获取网络金融服务身份认证信息五十组以上，一般用户身份认证信息二千五百组以上，或者侵入系统一百台以上，或者造成经济损失五万元以上的。）

（二）其他情节特别严重的情形。

提供侵入、非法控制计算机信息系统的程序、工具，明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

情节严重（285条）

10组

500组

20台

5000元/10000元

5倍

第二百八十五条 非法侵入计算机信息系统罪

违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。 违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。 提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。 单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

后果很严重

《刑法》第二百八十六条

【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

破坏计算机信息系统罪

行为	处罚	后果严重	后果特别严重
违反国家规定，对计算机**信息系统功能**进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行	后果严重—五年以下有期徒刑或者拘役 后果特别严重—五年以上有期徒刑	（一）造成10台以上计算机信息系统的主要软件或者硬件不能正常运行的； （二）对20台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的； （三）违法所得5000以上或者造成经济损失10000元以上的； （四）造成为100台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的； （五）造成其他严重后果的。	（一）数量或者数额达到前款第（一）项至第（三）项规定标准五倍以上的； （造成50台以上计算机信息系统的主要软件或者硬件不能正常运行的；对100台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的；违法所得25000元以上或者造成经济损失50000元以上的。） （二）造成为500台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的； （三）破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序，致使生产、生活受到严重影响或者造成恶劣社会影响的； （四）造成其他特别严重后果的。
违反国家规定，对计算机信息系统中存储、处理或者传输的**数据和应用程序**进行删除、修改、增加的操作			
故意**制作、传播计算机病毒等破坏性程序**，影响计算机系统正常运行			

情节严重（刑法-286条）

10台

20台

100台 / 1小时（一万用户）

5000元/10000元

5倍

第二百八十六条 破坏计算机信息系统罪

违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。 违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。 故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。 单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

情节严重（第285条）

10组

500组

20台

5000元/10000元

5倍

情节严重（第286条）

10台

20台

100台 / 1小时（一万用户）

5000元/10000元

5倍

后果很严重

《治安管理处罚法》

第二十九条　有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

（一）违反国家规定，侵入计算机信息系统，造成危害的；

（二）违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；

（三）违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

（四）故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的。

后果很严重

《网络安全法》

第六十三条 第三款　　违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。。

后果很严重

禁止性规定//事后性惩罚

刑事处罚//治安处罚//从业禁止

真爱必然克制

遵从法律框架、规范技术手段

真爱必然克制

恶意黑客X　　逃避打击X

以安全测试为目的所实施的漏洞挖掘有一定的合法行为空间√

真爱必然克制

《网络安全法》

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

一些建议

法律法规要加强学习
圈子里交友要谨慎
技术操作要规范

本章结束

~End~

但行好事，莫問前程。
Those that can, do.
Those that cannot,
complain.