数字应用基础

项目六：走进信息安全

项目6 走进信息安全

项目概述

本项目是一项旨在深化参与者对计算机网络与信息安全领域理解的综合性教育计划。本项目采用实践导向的教学模式，结合具体的任务与案例，使学员能够掌握信息安全的关键技术和策略，同时培养其在网络环境中处理数据、应对威胁和保护信息资产的能力。项目覆盖了计算机网络的基础知识，从网络的定义、组成、分类到安全设备的使用，再到网络协议和体系结构的理解。进一步深入至网络应用层面，包括WWW应用和电子邮件系统的安全使用，以及如何在互联网和专业数据库中高效检索信息。

项目分析

着重于培养参与者的信息安全意识，使他们能够识别和应对潜在的安全威胁。
项目按照任务和活动组织，每个任务包含若干个活动，形成由浅入深的学习路径，确保学员能够逐步掌握所需技能。
通过实训任务，学生能够在模拟环境中应用理论知识，提高实际操作能力。
学生将掌握网络设备配置、协议理解、数据加密与解密、安全防御与攻击技术等。

学习目标

认识计算机网络

理解计算机网络的基本概念、组成和分类，包括网络设备的功能和网络协议的作用

使用www与电子邮件

熟悉Web应用和电子邮件系统的工作原理及安全使用方法

使用安全工具设备

能够使用网络安全设备和工具，如防火墙、入侵检测系统等，进行基本的安全配置和监控

认识网络攻击

能够实施常见的安全防御策略，识别并应对网络攻击

信息检索技巧

掌握互联网信息检索技巧，包括使用搜索引擎和专业数据库

培养信息素养

具备信息安全的基础理论，包括信息安全威胁模型、防御机制和法规标准

建立信息安全意识

建立强烈的信息安全意识，能够识别并防范日常生活和工作中的安全风险

CONTENTS

目录

01 认识计算机网络

02 WWW应用

03 电子邮件应用

04 信息检索

05 培养信息安全素养

06 信息安全技术应用

01

认识计算机网络

任务6.1 认识计算机网络

任务描述

理解计算机网络的基础知识：从定义、组成部分、分类，到安全设备和协议体系，为学习者构建全面的网络认知框架。培养网络安全意识：通过介绍安全设备和网络协议，提高学习者在网络环境中的安全意识和防护能力。

任务分析

01. 学生应能描述计算机网络的定义、组成部分和分类

02. 应能识别并解释网络中关键的安全设备和协议的作用

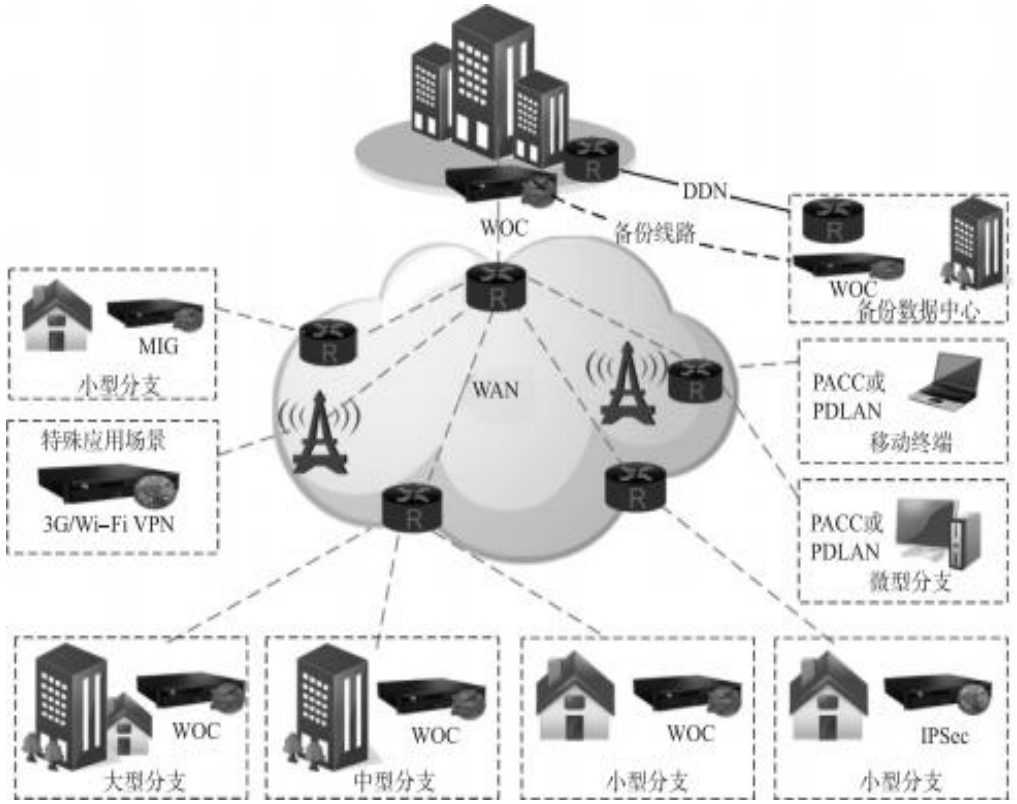
03. 能应用基本的网络知识和安全原则于现实场景中

活动1 计算机网络的定义

计算机网络，是指将地理位置不同的，具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。

从逻辑功能上看，计算机网络是以资源共享、传输信息为基础目的，用通信线路将多个计算机连接起来的计算机系统的集合。一个计算机网络组成包括传输介质和通信设备。

活动2 计算机网络的组成与分类



广域网示例图

- **计算机网络组成**

  包括计算机、网络操作系统、传输介质及应用软件。

- **网络类型划分**

  按地理范围分为局域网、城域网、广域网和互联网。

活动2 计算机网络的组成与分类

1.局域网(LAN)

通常常见的“LAN”就是指局域网，这是最常见、应用最广的一种网络。局域网随着整个计算机网络技术的发展和提高而得到充分的应用和普及，几乎每个单位都有自己的局域网，有的甚至家庭中都有自己的小型局域网。所谓局域网，那就是在局部地区范围内的网络，它所覆盖的地区范围较小。局域网在计算机数量配置上没有太多的限制，少的可以只有两台，多的可达几百台。一般来说，在企业局域网中，工作站的数量在几十到两百台次左右。在网络所涉及的地理距离上，一般来说，是几米至10km。局域网一般位于一个建筑物或一个单位内，不存在寻径问题，不包括网络层的应用。

2.城域网(MAN)

城域网多采用ATM技术做骨干网。ATM是一个用于数据、语音、视频及多媒体应用程序的高速网络传输方法。ATM包括一个接口和一个协议，该协议能够在一个常规的传输信道上，在比特率不变及变化的通信量之间进行切换。ATM也包括硬件、软件及与ATM协议标准一致的介质。ATM提供一个可伸缩的主干基础设施，以便能够适应不同规模、速度及寻址技术的网络。ATM的最大缺点就是成本太高，所以一般在政府城域网中应用，如邮政、银行、医院等。

3.广域网(WAN)

这种网络也称为远程网，所覆盖的范围比城域网(MAN)的更广，它一般是在不同城市之间的LAN或者MAN网络互联，地理范围可从几百千米到几千千米，如图5 - 2所示。因为距离较远，信息衰减比较严重，所以这种网络一般要租用专线，通过IMP(接口信息处理)协议和线路连接起来，构成网状结构，解决循径问题。

4.互联网

互联网(internet)，又称网际网络，始于1969年美国的阿帕网，是网络与网络之间所串联成的庞大网络。这些网络以一组通用的协议相连，形成逻辑上的单一巨大国际网络。互联网是世界上最大的广域网。

活动3 网络通信组件----通信介质

同轴电缆

同轴电缆从用途上可以分为基带同轴电缆和宽带同轴电缆(即网络同轴电缆和视频同轴电缆)。

双绞线

双绞线有两种基本类型：屏蔽双绞线(STP)和非屏蔽双绞线(UTP)，它们都是由两根绞在一起的导线形成传输电路。

光纤

光纤具有圆柱形的形状，由三部分组成：纤芯、包层和护套。纤芯是最内层部分，它由一根或多根非常细的由玻璃或塑料制成的绞合线或纤维组成。

无线介质

不使用导线，这就是无线电通信。无线电通信利用电磁波或光波来传输信息。

活动3 网络通信组件----网络设备

交换机(Switch)

xDSL路由器

集线器

路由器(Router)

网络适配器

活动4 网络协议与体系结构

1.网络协议体系结构

在计算机网络中要做到有条不紊地交换数据，就必须遵守一些事先约定好的规则。这些规则明确规定了所交换的数据格式及有关的同步问题。这里所说的同步不是狭义的(即同频或同频同相)，而是广义的，即在一定的条件下应当发生什么事件(如发送一个应答信息)，因而同步含有时序的意思。这些为进行网络中的数据交换而建立的规则、标准或约定称为网络协议，网络协议也可简称为协议。

网络协议主要由三个要素组成

①语法，即数据与控制信息的结构或格式。

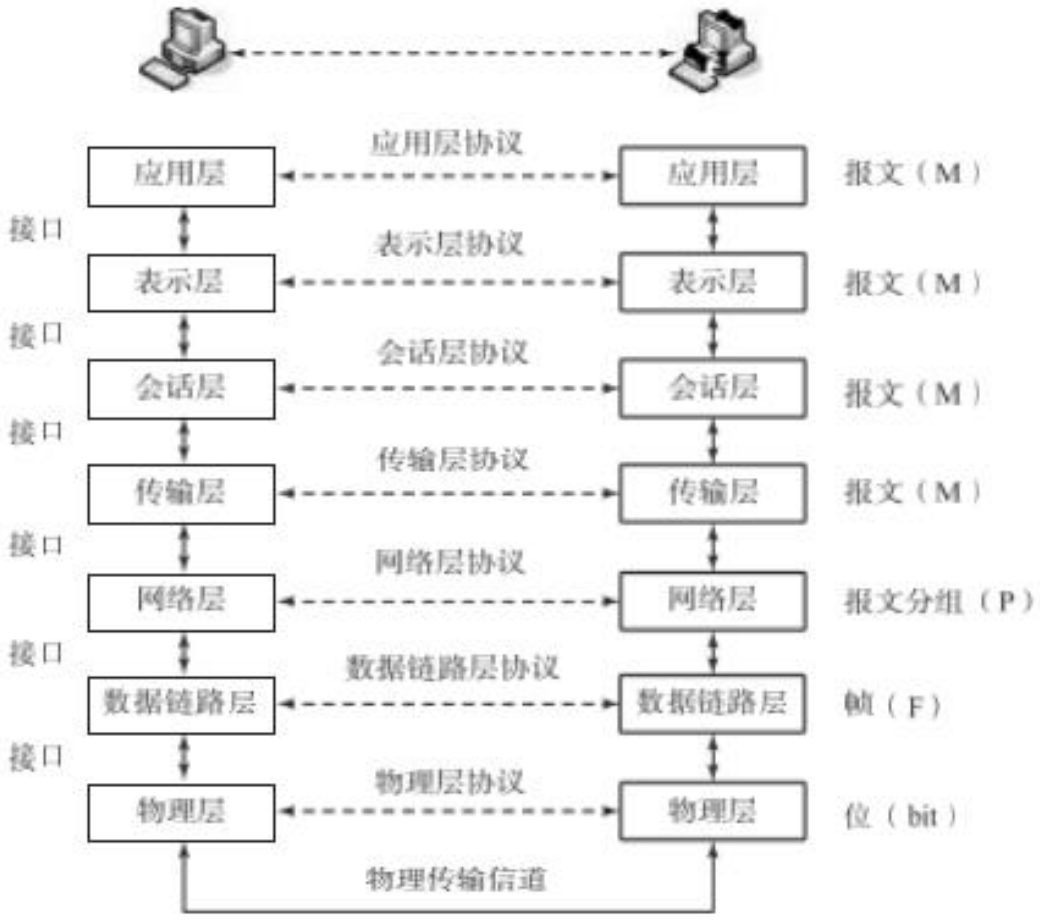
②语义，即需要发出何种控制信息，完成何种动作及做出何种响应。

③同步，即事件实现顺序的详细说明。

网络协议是计算机网络的不可缺少的组成部分。协议通常有两种不同的形式：一种是使用便于人来阅读和理解的文字描述，另一种是使用计算机能够理解的程序代码。

活动4 网络协议与体系结构----OSI参考模型

开放系统互连(OSI)参考模型采用分层的结构化技术，共分为7层，从低到高为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。无论什么样的分层模型，都基于一个基本思想，遵守同样的分层原则：目标站第N层收到的对象应当与源站第N层发出的对象完全一致。



活动4 网络协议与体系结构----OSI参考模型

提供应用程序间的网络服务。
包括建立连接、同步和错误处理。

负责数据格式转换和加密。
实现不同计算机系统间的互操作性。

建立、管理和终止会话。
支持同步点以恢复会话。

确保端到端的数据传输可靠性。
使用错误和流量控制机制。

负责路由选择和寻址，确保数据包跨网络传输。
处理拥塞控制和异构网络互连。

提供相邻节点间可靠的数据传输。
将数据封装成帧，并包含错误和流量控制。

管理比特流在物理介质上的传输。
定义机械、电气、功能和规程特性。

活动4 网络协议与体系结构----TCP/IP参考模型

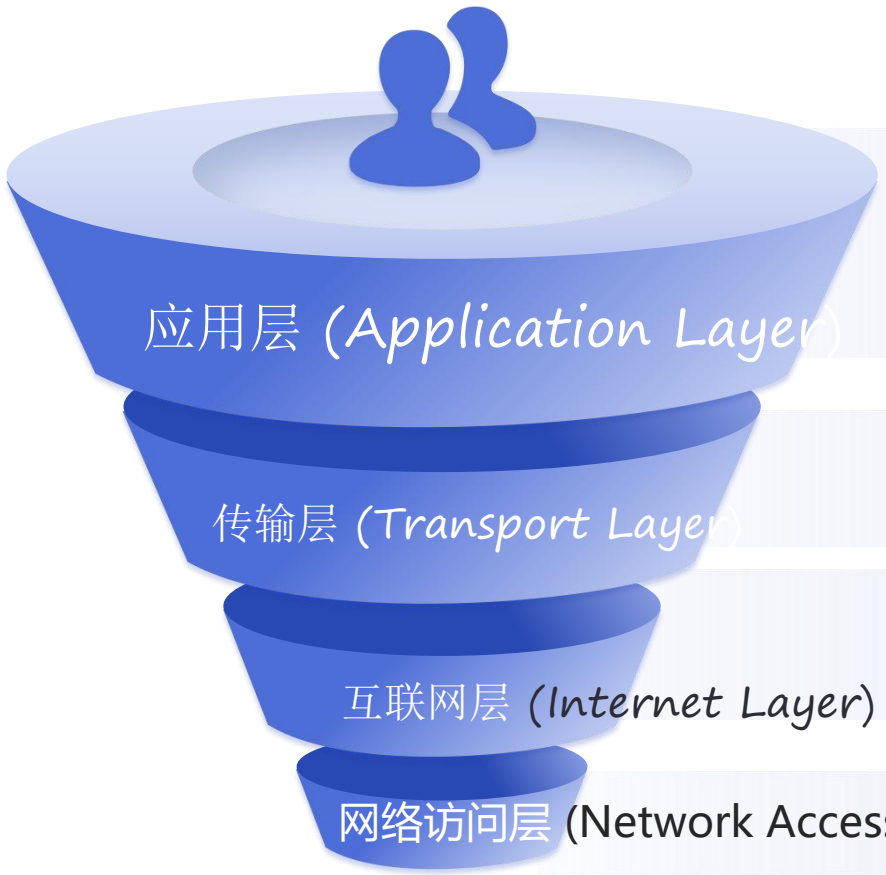
TCP / IP模型

前面已讲述了七层协议OSI参考模型，TCP / IP模型及其协议族使得世界上任意两台计算机间的通信成为可能。

TCP / IP参考模型

TCP / IP参考模型是首先由ARPANET所使用的网络体系结构。这个体系结构在它的两个主要协议出现以后被称为TCP / IP参考模型(TCP / IPReferenceModel)。这一网络协议共分为四层：网络访问层、互联网层、传输层和应用层.

活动4 网络协议与体系结构----TCP/IP参考模型



包含所有高层协议。示例协议:
TELNET: 远程登录。FTP: 文件传输。
SMTP: 电子邮件传输。DNS: 主机名解析。
NNTP: 新闻传输。HTTP: Web页面传输。

支持源端和目的端之间的会话。
定义 TCP 和 UDP 协议。

关键层，支持分组在网络间的传输。
使用 IP 协议进行寻址和路由选择。
分组可能通过不同的路径到达，顺序可能不同。

负责主机与网络之间的物理连接。
功能由网卡或调制解调器完成。

活动4 网络协议与体系结构----OSI和TCP/IP模型比较

相似点

都采用了层次化结构，有传输层、网络层和应用层，都是基于协议数据单元的分组交换网络。

不同点

OSI有7层，TCP/IP有4层；TCP/IP无表示层和会话层，OSI支持无连接和面向连接服务，TCP/IP网络层仅支持无连接。

02

www应用

任务6.2 WWW应用

任务描述

在数字化时代，WorldWideWeb（简称WWW或Web）已成为人们获取信息、沟通交流和开展业务的重要平台。本任务旨在让学习者深入了解Web的工作原理，掌握使用Web浏览器的技能，以及利用Web进行高效信息检索的方法。通过以下活动，我们将引导学习者从理论到实践，全面掌握WWW应用的各个方面。

任务分析

01 **搜索引擎使用技巧**

利用关键词、引号、减号等提高搜索精度，使用高级搜索功能，筛选结果。

02 **专业数据库访问**

了解并访问学术、行业等专业数据库，利用布尔逻辑、字段限定等高级搜索技巧。

03 **浏览器基础操作**

掌握地址栏输入、书签管理、隐私模式等基本操作，提升浏览效率。

04 **扩展程序管理**

安装浏览器扩展程序，如广告拦截、翻译等，提升浏览体验。

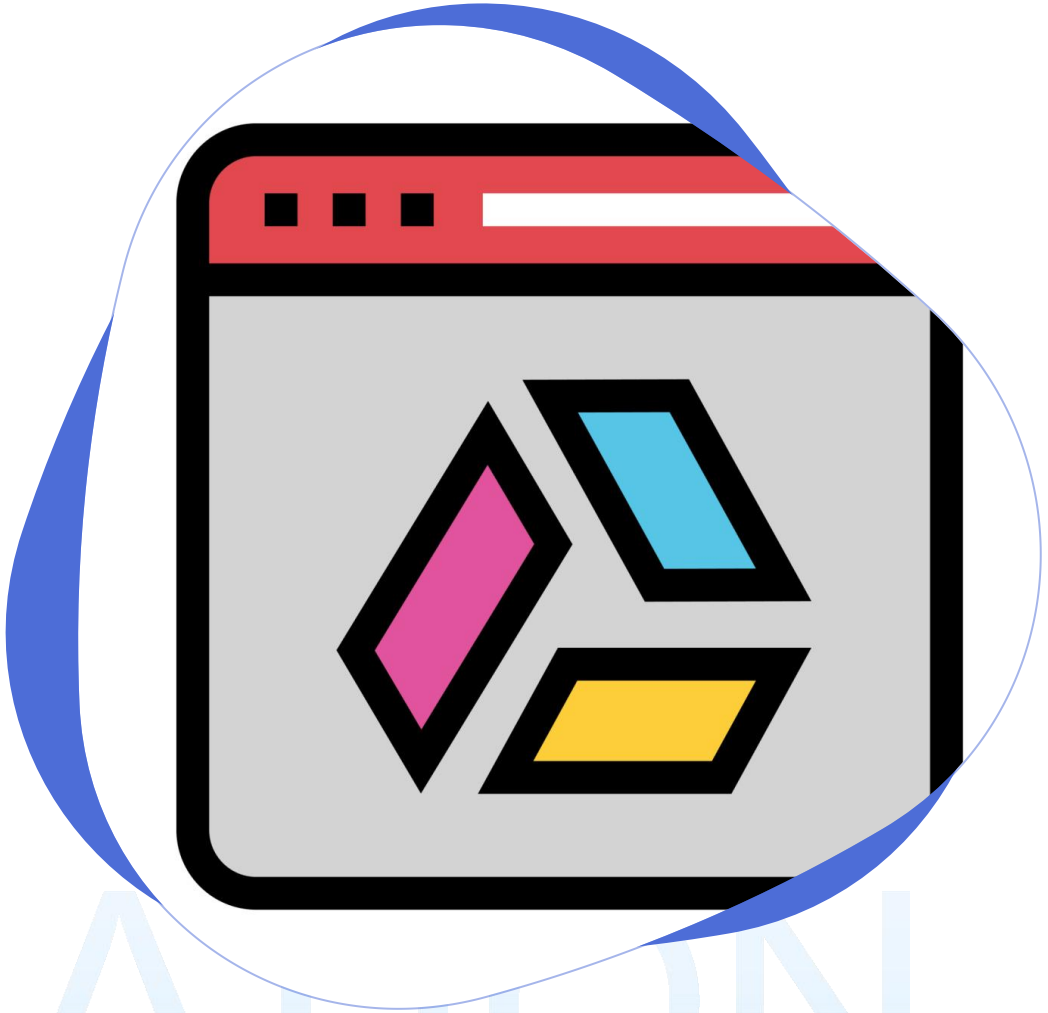
05 **网页保存与打印**

学会保存网页为PDF、图片等格式，以及打印网页内容，便于后续查阅。

活动1 浏览器的介绍

浏览器的基本概念

浏览器是软件应用程序，用于检索、解析和显示WWW内容，支持多媒体、Web应用、在线购物等。



发展历程

浏览器历史始于1990年代初，经历了Mosaic、NetscapeNavigator、IE等阶段，GoogleChrome发布后成为最受欢迎浏览器之一。

活动1 浏览器的介绍----主流浏览器介绍

01 GoogleChrome

Google开发，基于Chromium，速度快且稳定，支持扩展程序，集成Google服务，多设备同步，隐私保护强。

02 MozillaFirefox

Mozilla基金会开发，开源，Gecko引擎，Quantum引擎提升性能，保护隐私和互联网自由，扩展丰富。

03 MicrosoftEdge

Windows默认浏览器，新版基于Chromium，集成Microsoft服务，隐私安全功能强，支持垂直标签页和PDF阅读。

04 AppleSafari

苹果公司产品，WebKit引擎，界面简洁，电池寿命优化，隐私保护严格，包括智能防跟踪和加密通信。

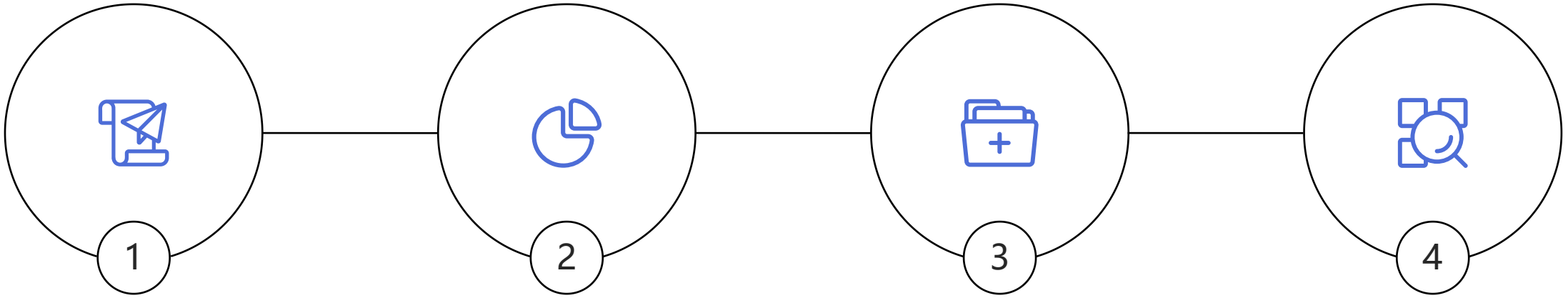
05 Opera

历史悠久的浏览器，创新功能多，基于Chromium，内置广告拦截、VPN和加密货币钱包，保护用户安全。

06 OtherNotableBrowsers

Brave：隐私为中心，广告拦截和加密货币奖励；Vivaldi：高度可定制，适合高级用户；TorBrowser：基于Firefox，匿名浏览。

活动1 浏览器的介绍----IE浏览器的发展历程



IE简介

InternetExplorer是微软公司开发的Web浏览器，自1995年起成为Windows标准浏览器。

主要版本

IE3引入Java和ActiveX；IE4整合到Windows98；IE5提供离线浏览；IE6是XP默认浏览器；IE7增标签页浏览；IE8引入私密浏览；IE9提升JavaScript；IE10优化Windows8；IE11支持现代Web标准。

特点与功能

集成性：与Windows深度集成；兼容性：支持多种Web标准；安全性：加强安全功能；隐私保护：InPrivate浏览模式；插件支持：丰富功能但增加安全风险。

当前状况

微软于2022年6月15日停止对IE所有版本的支持，但MicrosoftEdge包含IE模式以兼容旧网站和企业应用。

活动2 浏览器常用功能介绍

输入网址或搜索查询，访问网页或执行搜索，智能提示，自动补全已访问过的网址或搜索历史。

保存喜爱的网站，方便快速访问，支持书签整理、分组、搜索和同步到其他设备。

在浏览历史中向前或向后移动，快速回到之前的页面，通常位于浏览器界面的左上角。

重新加载当前页面，获取最新的内容，通常与地址栏相邻，有时与停止加载按钮共享图标。

同时打开和管理多个网页，提高多任务处理能力，支持在同一个浏览器窗口中切换不同的网页，支持标签页拖拽、分组和恢复已关闭的标签页。

浏览时不保存历史记录、Cookies和临时文件，保护隐私，在隐私模式下，浏览器不会记住用户在该模式下的活动。

活动2 浏览器常用功能介绍

用途：查看和搜索访问过的网页记录。特性：按时间、关键字或访问频率排序，支持清除历史记录。

用途：控制浏览器的安全级别，设置隐私保护选项。特性：允许用户自定义安全和隐私偏好，如启用防钓鱼和防恶意软件保护。

用途：管理网页上的文件下载，查看下载进度。特性：暂停、恢复和取消下载，显示下载历史。

用途：扩展浏览器功能，如广告屏蔽、密码管理、生产力工具等。特性：通过浏览器的扩展商店下载和安装，可自定义界面和功能。

用途：用于网页开发和调试，检查网页元素，查看网络请求。特性：包括元素检查器、控制台、网络监控、性能分析和源代码编辑器。

活动3 浏览器的使用----浏览Web页

01

输入网址浏览网页

在地址栏输入网址，按Enter键进入网站浏览。

02

采用超链接功能浏览网页

鼠标单击超链接点跳转至目标网页，快捷简便。

03

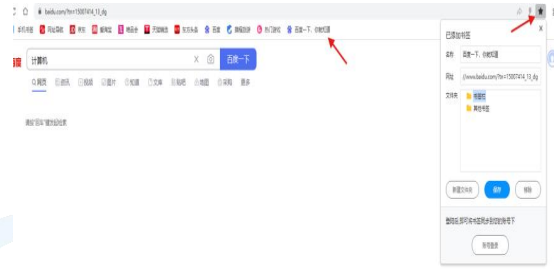
使用搜索引擎搜索互联网信息

通过搜索引擎输入关键字，检索并浏览相关信息。

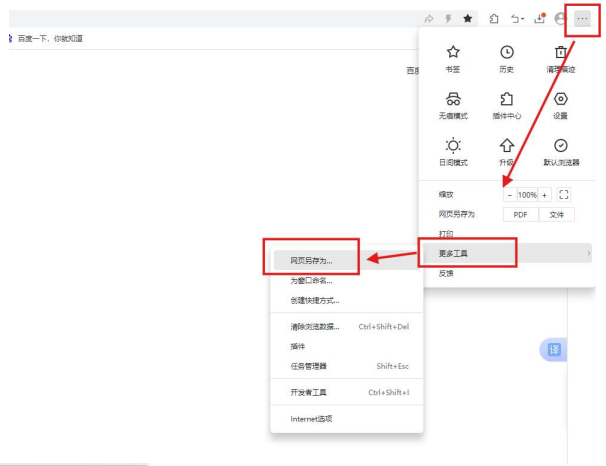
04

使用收藏夹访问网页

将常用网页地址添加到收藏夹，快速访问。



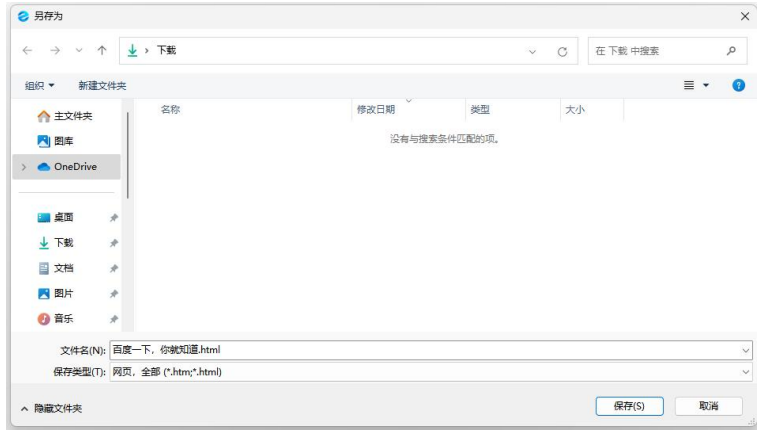
活动3 浏览器的使用-------保存当前页面



01

保存当前访问网页

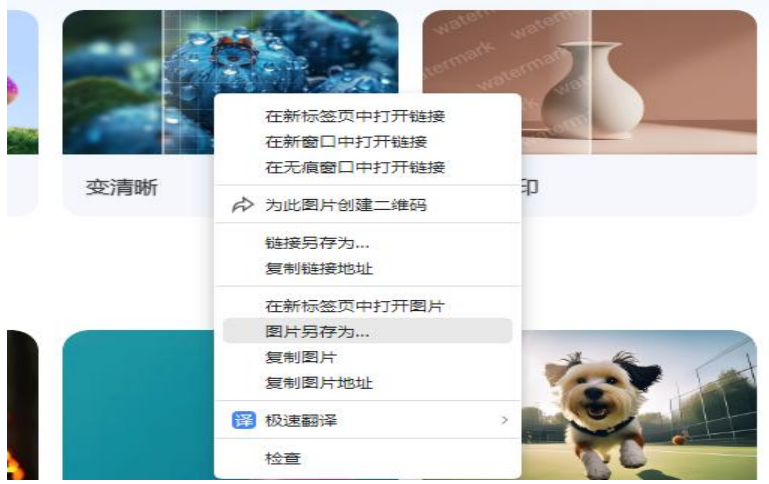
选择“设置”→“更多工具”→“网页另存为”，确定保存位置、文件名和类型，单击“保存”。



02

保存网页中的图片

右击需要保存的图片，选择“图片另存为”命令即可。



03

电子邮件应用

任务6.3 电子邮件应用

任务描述

电子邮件（E-mail）作为一种基本的网络通讯工具，在日常沟通、商务交流和信息传递中扮演着至关重要的角色。本任务旨在使学习者掌握电子邮件的基础知识，学会申请和使用电子邮件账户，以及有效地撰写、发送和管理邮件。通过以下活动，我们将引导学习者从理论到实践，全面掌握电子邮件应用的各个环节。

任务分析

01 **电子邮件基本概念**

电子邮件是电子通信方式，通过计算机网络发送和接收信息。

02 **电子邮件历史与技术**

电子邮件起源于20世纪70年代，基于SMTP、POP3等技术标准。

03 **申请与设置账户**

在邮箱服务商网站注册，设置账户信息，配置客户端或网页版。

04 **撰写与发送邮件**

编写邮件主题、正文，添加附件，选择收件人，点击发送。

05 **接收与管理邮件**

登录邮箱，查看收件箱，分类整理邮件，删除或归档。

06 **邮件安全保护**

设置强密码，定期更换，警惕网络钓鱼，防范垃圾邮件和恶意软件。

活动1 电子邮件的知识

01

电子邮件简介

电子邮件是Internet中应用最广的服务，可快速、低廉地与世界各地用户联络，支持文字、图像、声音等形式。

02

电子邮件服务协议

SMTP用于邮件传送，POP3用于邮件下载，两者共同构成电子邮件系统的基础。

03

邮件结构

邮件包括发件人、收件人、抄送、密送、主题、正文和附件等部分，共同构成完整的邮件内容。

INFORMATION

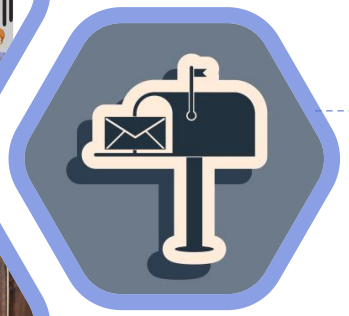
活动2 电子邮箱的申请和使用方法

电子邮箱概述

电子邮箱是邮件服务器为每个注册用户提供的有限存储空间，用于存储电子邮件。

电子邮箱的注册

用户到ISP处办理上网账户时，通常会同时获得电子邮箱。



电子邮箱地址的构成

E-mail地址由用户名、@符号和邮件服务器名组成，如user@sina.com.cn。

电子邮箱的工作原理

电子邮件按照POP协议被传送到邮件服务器上，再按SMTP协议转发到用户计算机上。

电子邮箱服务提供商

网易、新浪、搜狐等门户网站提供免费电子邮箱服务，支持万维网方式在线收发。

活动2 电子邮箱的申请和使用方法

填写基本信息

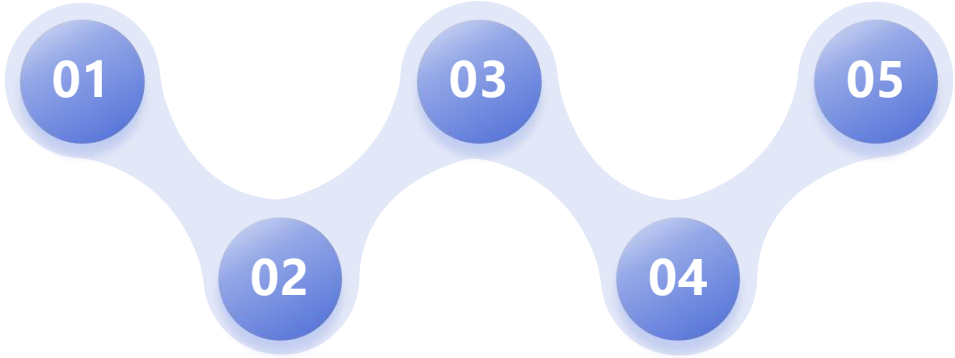
填写邮件地址、密码、验证码，邮件地址需6~18个字符，以字母开头，密码需8~16个字符，含大小写字母和数字。

短信验证

使用手机微信或摄像头扫描二维码，编辑短信发送至对应收件人，完成验证。

进入邮箱

在注册成功页面中点击“进入邮箱”按钮，进入邮箱页面，完成邮箱申请。



手机号码验证

手机号码不能为空，需填写正确手机号。

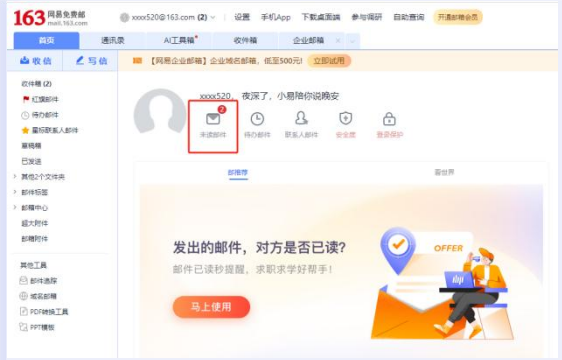
注册成功

单击“立即注册”按钮，显示注册成功页面。

活动2 电子邮箱的申请和使用方法

进入免费邮箱首页

在地址栏中输入网址：www.163.com，点击登录按钮，根据邮箱账号或手机账号登录。



查看邮件

在收件箱中看到2封未读邮件。

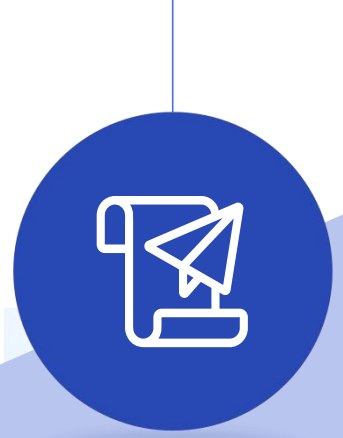
进入收件箱页面

单击“收件箱”或“未读邮件”按钮，进入收件箱页面。

阅读电子邮件

单击需要阅读的电子邮件主题链接，在新网页中打开该电子邮箱。

活动2 电子邮箱的申请和使用方法



打开写信界面

在邮件首页单击“写信”按钮，打开“写信”界面。

填写收件人和主题

在“收件人”一栏填写收件人地址，用“,”隔开多个收件人。填写邮件主题。

添加附件

单击“添加附件”超链接，选择文件并单击“打开”按钮。重复操作添加多个附件，删除附件则单击“删除”按钮。

编写邮件内容

在正文窗口填写信件内容，使用工具栏按钮美化字体，插入信纸、图片等。

发送邮件

邮件完成后，单击“发送”按钮，查看发送成功提示。单击“已发送”超链接查看已发送邮件。

04

信息检索

任务6.4 信息检索

任务描述

信息检索是一项复杂而精细的任务，旨在从海量的数据集中精准定位用户所需的信息。这一过程始于用户发出的查询，可能是关键词、短语或自然语言问题的形式。系统接收到查询后，会通过一系列算法和技术，在数据库或互联网上搜索与查询相匹配的文档或数据。信息检索的核心在于理解查询意图、索引和检索文档、评估相关性，并最终返回最符合用户需求的结果。此外，系统还需具备反馈机制，能够根据用户的行为和反馈持续优化检索效果，提升用户体验。

任务分析

01 **构建有效搜索查询**

学习如何构建有效的搜索查询，利用高级搜索语法提高搜索精度。

02 **分类统计**

分类统计，通过细致的分类和统计，可以更好地了解和管理资源。

03 **文献管理工具使用**

利用文献管理工具，参与者将学会如何系统地组织和引用文献，对撰写论文和报告至关重要。

活动1互联网信息检索

活动情景

小王现在已经是一名大学生啦，虽然每个月，爸爸妈妈都按时给他生活费，但是他还想暑假的时候能去一直向往的云南走走，这个花费他就不好意思管爸妈伸手。正在这时，他收到一条来自陌生号码的短信：

“***信息科技有限公司招兼职啦！只要能识字，只要有一台手机即可，每天一小时，每月轻松增加收入2000元。”看到这条短信之后，小王非常心动。但是，又觉得这种天上掉馅饼的事情不知道是否可靠。现在他想通过信息检索来确认这条短信到底是正常的招聘信息还是诈骗信息。

活动分析

要知道这条招聘信息是否靠谱，可以借助互联网的力量。使用浏览器可以对互联网进行访问。而如果要对特定的内容进行检索，则需要用到搜索引擎。本案例中，想知道招聘信息是否靠谱，可以从如下几个方面对招聘信息进行检索：

（1）招聘的企业是否合法合规

（2）从事的工作是否合法合规

（3）工作和收入是否合理。

活动1 互联网信息检索----检索流程

01 检索内容概述

确认招聘信息真伪，需从招聘企业合法性、工作合法性、工作和收入合理性三方面进行检索。

02 选择搜索引擎

根据搜索内容，选择百度搜索引擎进行信息检索。

03 打开浏览器

单击【开始】按钮，选择【MicrosoftIE】或双击桌面IE浏览器快捷方式打开浏览器。

04 访问百度搜索引擎

在IE浏览器地址栏输入www.baidu.com，打开百度搜索引擎。

05 搜索官方企业信用系统

在百度搜索栏输入“国家企业信用信息公示系统”，点击官方链接进入。

06 查找企业信息

在公示系统搜索栏输入企业名称或相关代码，点击查询获取企业信息。

活动1互联网信息检索----杜绝诈骗发生的方法

避免点击不明链接

不要点击不明来源的网络连接，以防被诈骗。

保护个人信息

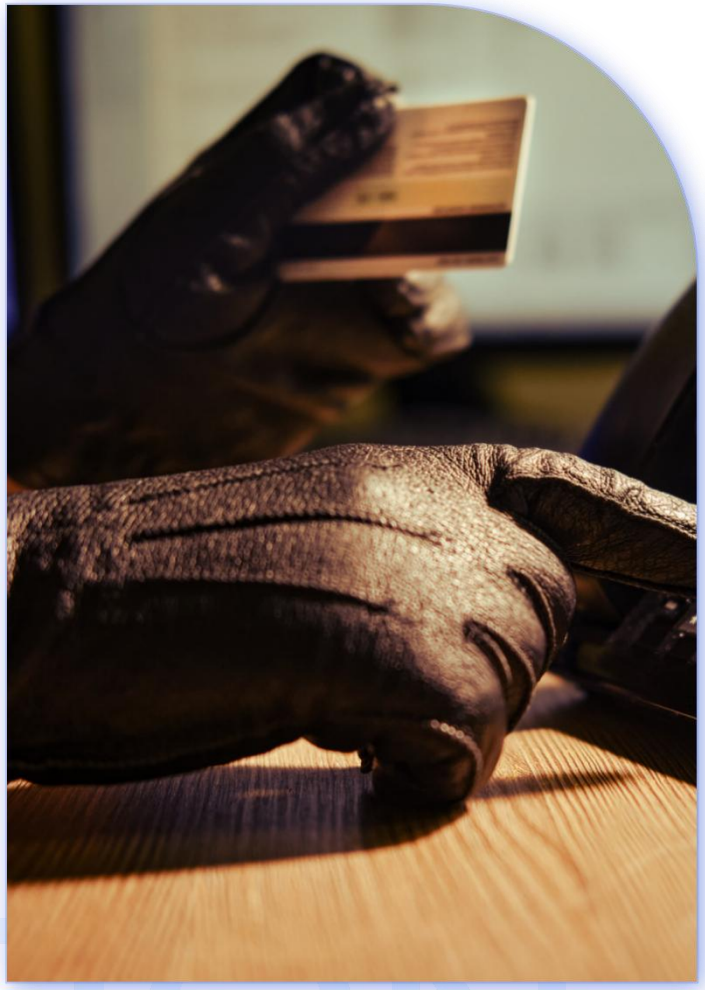
不要随意泄露自己个人信息，避免被不法分子利用。

不泄露验证码

不能将自己手机收到的短信验证码告诉他人，防止被诈骗。

警惕资金要求

遇到对方要求交押金，垫付资金等涉及到资金的情况直接认定对方为诈骗。



活动2 文献检索实践

活动情景

小王现在已经是一名大学生了，期末的时候，老师留了一个作业：写一篇有关我国计算机发展历史的论文，要求数据真实可靠。

活动分析

老师布置的这个作业要求对计算机的发展历史有相当的了解，通过搜索引擎可以搜索到很多信息，但是，信息的区分，分类等等都是难题。为了获得准确、完整的数据，需要进行文献检索。

活动2 文献检索实践----活动实施

01 课题分析确定主题概念

明确文献检索目的、实质问题、主题概念关系、学科范围、语种时间范围等。

02 选择检索方式和数据库

考虑专业性、权威性、收录范围、检索方法及系统功能，选用知网作为检索系统。

03 确定检索途径

根据题目要求，选用“主题”进行检索，提炼出关键词如计算机发展、电脑发展等。

04 构造检索式

由检索词和组配算符构成检索式，注意同义词或近义词之间用“逻辑或”组配。

05 检索策略的反馈调整

如检索结果不理想，可从检索词准确性、运算符使用、检索途径等方面进行调整。

06 检索结果的处理

直接查阅或下载存盘，并在论文参考文献列表中列出。

05

培养信息安全素养

任务6.5 培养信息安全素养

任务描述

21世纪是信息的社会。信息是社会发展的重要战略资源，也是衡量国家综合国力的一个重要参数。信息作为继物质和能源之后的第三类资源，它的价值日益受到人们的重视。信息的地位与作用因信息技术的快速发展而急剧上升，信息安全的问题同样因此而日渐突出。信息的泄露、篡改、假冒和重传、黑客入侵、非法访问、计算机犯罪、计算机病毒传播等对信息网络已构成重大威胁，这些都是当前计算机安全必须面对和解决的实际问题。本章主要介绍信息安全基本概念、信息安全防范技术、网络安全技术、计算机病毒等内容。

任务分析

01 **关键概念认知**

学生能解释信息安全的关键概念，并认识到其重要性。

02 **信息资产保护**

能够自觉采取措施保护自己的信息资产。

03 **网络威胁识别与防范**

能够识别常见的网络威胁，并了解如何防范。

04 **机构安全等级保护**

了解自己所在机构应采取的安全等级保护措施。

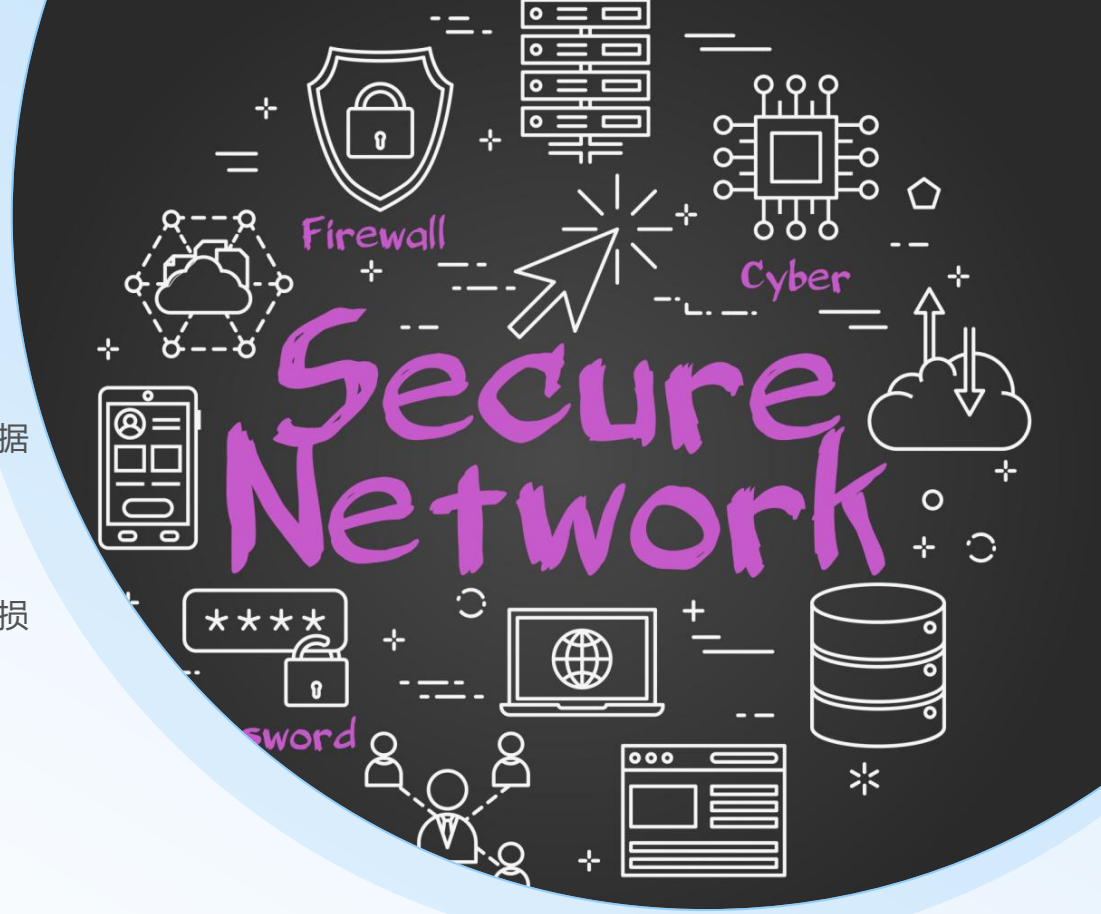
05 **病毒防护能力**

能够识别病毒迹象并采取适当措施进行防护。

06 **信息安全架构理解**

能够理解信息安全架构的关键组成部分，并能够在一定程度上应用这些知识。

活动1 掌握信息安全基本概念



01 信息安全定义

信息安全指为数据处理系统建立的技术、管理上的安全保护，保护计算机硬件、软件、数据不因偶然和恶意原因破坏、更改和泄露。

02 信息安全的重要性

信息作为重要资产需受保护，信息安全与每个人权益息息相关，隐含缺陷、失误可致巨大损失。

03 信息安全的范围

信息安全范围广泛，包括防范商业机密泄露、青少年不良信息浏览、个人信息泄露等。

04 信息安全的学科基础

信息安全是综合性学科，涉及计算机科学、网络技术、通信技术、密码学等多门学科。

05 信息安全与网络安全的关系

信息安全以网络安全为基础，但两者有区别，网络绝对安全也不能完全保障信息安全。

06 信息安全等级

信息安全从下至上有计算机密码安全、局域网安全、互联网安全和信息安全之分，涉及保密性、完整性、可用性、可控性、不可否认性。

活动1 掌握信息安全基本概念

01 信息系统安全概述

信息系统的安全是指存储信息的计算机、数据库系统的安全和传输信息网络的安全。

02 计算机系统安全

计算机系统安全指保护计算机软件、硬件和数据资源不被更改、破坏及泄露。

03 数据库系统安全

数据库面临的安全威胁主要有数据库文件安全、未授权用户窃取、修改数据库内容、授权用户的误操作等。

04 信息传输系统安全

信息传输系统的主要安全任务是保证信息能正确传输并防止信息泄露、篡改与冒用。

05 信息安全与信息系统安全的关系

信息安全依赖于信息系统的安全，确保信息系统的安全是保证信息安全的手段。

活动1 掌握信息安全基本概念----信息安全的目标与原则

01 信息安全的目标

保密性：确保信息仅被授权的个人或实体访问，通过加密、访问控制等手段实现。

完整性：保证信息不被未经授权的修改或破坏，使用数字签名、哈希函数等技术验证。

可用性：确保信息和信息系统对授权用户始终可用，涉及灾难恢复计划、冗余系统等措施。

02 信息安全的原则

最小特权原则：用户或程序只能获得完成其任务所需的最少权限。

纵深防御：采用多层防护措施保护信息资产，即使某一层被突破，还有其他层保护。

安全生命周期：将安全考虑贯穿于信息系统的整个生命周期，从设计到退役。

活动1 掌握信息安全基本概念----信息安全的任务

01

保障信息系统安全

建立可靠的数据存储冗余备份，确保数据灾难恢复。

02

建立访问控制机制

单击此处输入你的项正文，文字是您思想的提炼。单击此处输入你的项正文，文字是您思想的提炼

03

数据加密

单击此处输入你的项正文，文字是您思想的提炼。单击此处输入你的项正文，文字是您思想的提炼

04

系统升级与修补

单击此处输入你的项正文，文字是您思想的提炼。单击此处输入你的项正文，文字是您思想的提炼

05

安装防火墙

单击此处输入你的项正文，文字是您思想的提炼。单击此处输入你的项正文，文字是您思想的提炼

活动2 建立信息安全意识

信息安全意识定义

信息安全意识是信息化工作中对可能损害信息的外在条件的戒备和警觉心理状态。

信息安全意识的重要性

树立良好信息安全意识，认知安全问题，恪守正确行为方式，清楚应对措施。

活动2 建立信息安全意识----常见的网络欺诈行为

1

网络欺诈定义

网络欺诈指不法分子通过电话、网络或手机短信，编造虚假信息，设置骗局，骗取受害人利益。

网络欺诈特点

网络欺诈具有隐蔽性、多样性、产业化、跨地域等特点。

2

INFORMATION

活动2 建立信息安全意识----常见的网络欺诈行为

1

虚假中奖欺诈

编造虚假中奖信息，诱骗受害人支付费用或提供个人信息。

2

冒充亲友欺诈

冒充受害人亲友，编造紧急情况，骗取受害人钱财。

3

征婚交友欺诈

通过征婚交友平台，建立虚假关系，骗取受害人信任后实施欺诈。

4

网络购物欺诈

在网络购物平台上发布虚假商品信息，诱骗受害人支付货款后消失。

5

就业招聘欺诈

发布虚假招聘信息，骗取受害人求职费用或个人信息。

6

网络钓鱼诈欺诈

通过伪装成合法网站或邮件，诱骗受害人输入敏感信息，如账号密码等。

7

私募基金欺诈

以私募基金名义非法集资，骗取受害人投资款。

8

炒股暴富欺诈

编造炒股暴富信息，诱骗受害人投资或支付高额咨询费用。

9

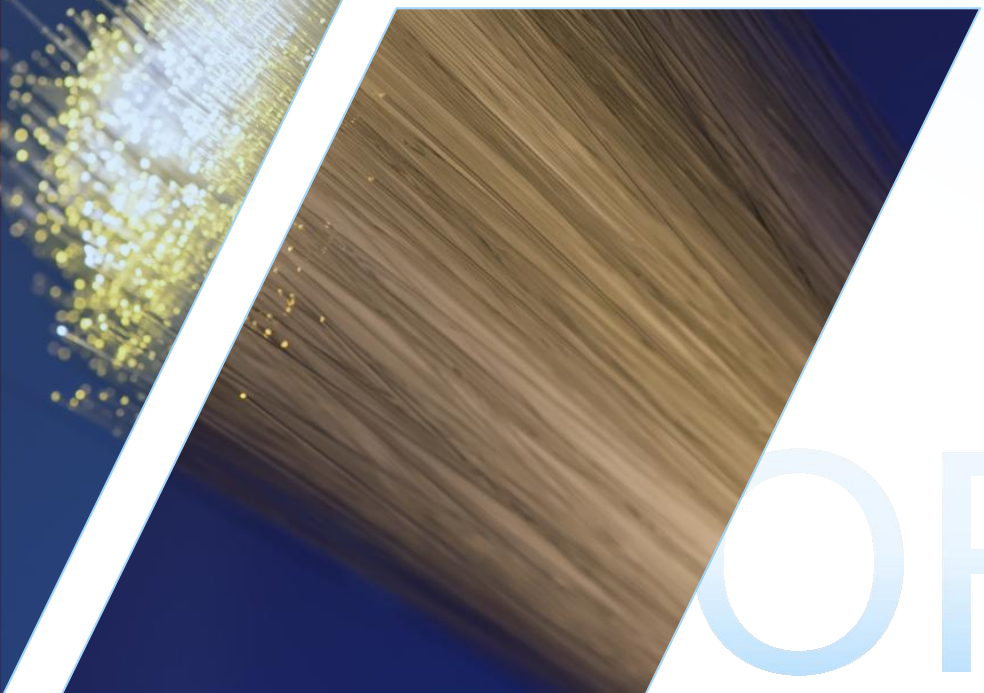
彩票预测欺诈

编造彩票预测信息，诱骗受害人购买彩票或支付预测费用。

10

网游装备欺诈

在网游中出售虚假装备或账号，骗取受害人钱财。



活动2 建立信息安全意识----信息系统的不安全因素

信息存储

信息存储需可靠措施，以防意外丢失数据造成损失，存储设备故障需数据备份技术保障信息完整性。

信息通信传输威胁

信息通信传输面临被动和主动攻击威胁，被动攻击如监视明文，主动攻击如篡改数据、破坏系统、拒绝服务等。

ORMATION

活动3 了解信息安全威胁

网络信息安全问题

计算机网络，特别是互联网，提供便利的同时，网络信息安全问题日渐突出。

TCP/IP协议的安全隐患

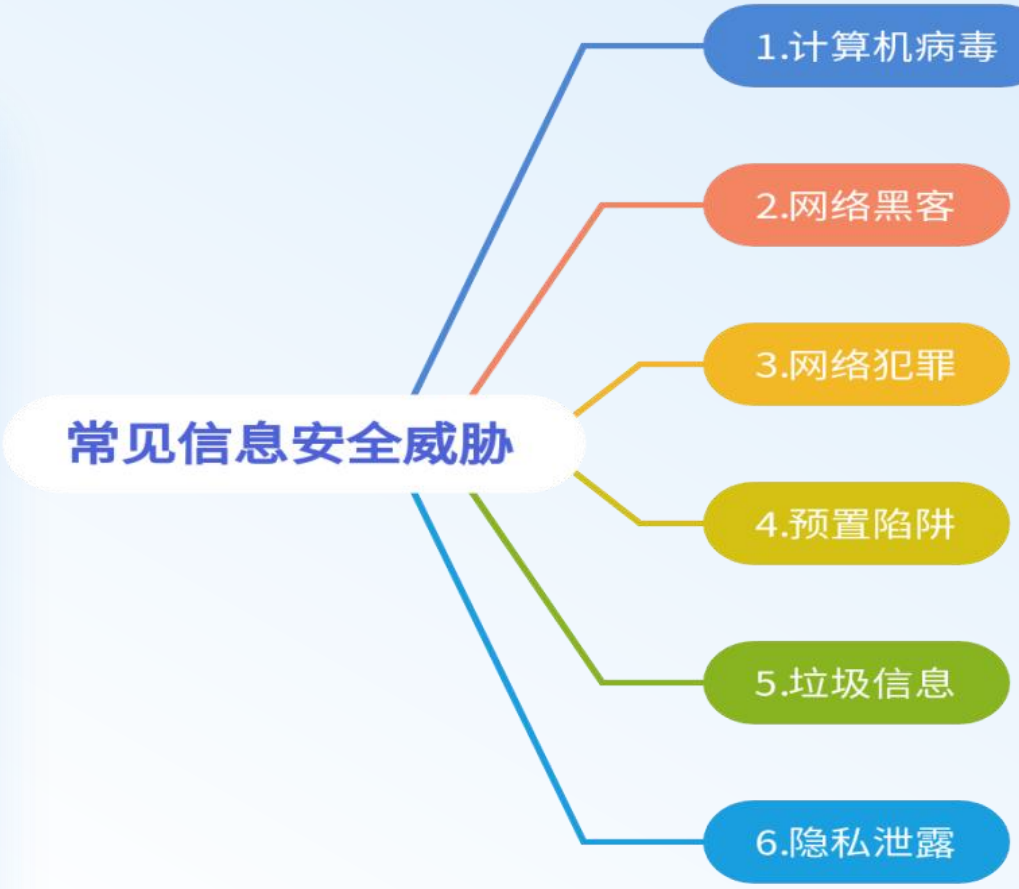
TCP/IP设计时未考虑安全问题，存在信息泄露、窃取篡改、行为否认、授权侵犯等隐患。

协议不安全性与黑客攻击

网络中协议的不安全性为黑客提供了方便，黑客利用系统缺陷或漏洞进行攻击。

常见安全威胁

信息安全威胁多样，包括端口扫描、网络窃听、拒绝服务、TCP/IP劫持等。



活动4 认识网络安全等级保护

01

定义

信息安全等级保护是对信息和信息载体按重要性等级保护的工作。

02

网络安全等级保护

对网络实施分等级保护、监管，安全产品分等级管理，安全事件分等级响应、处置。

03

基本原则

包括明确责任，共同保护；依照标准，自行保护；同步建设，动态调整；指导监督，重点保护。

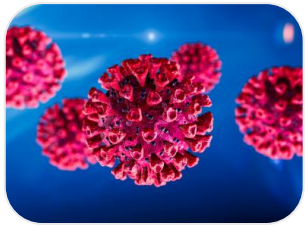
活动5 认识计算机病毒----计算机病毒的定义与特性

计算机病毒的定义

计算机病毒是破坏计算机功能或数据，能自我复制的一组计算机指令或程序代码。

计算机病毒的特性

计算机病毒是程序，具有传染性，通过修改其他文件传播，非自然生命体，运行消耗资源。



计算机病毒的目的

多数病毒目的是毁坏数据，但也有恶作剧病毒仅显示有趣消息或画面。

活动5 认识计算机病毒----计算机病毒的产生

计算机病毒的起源

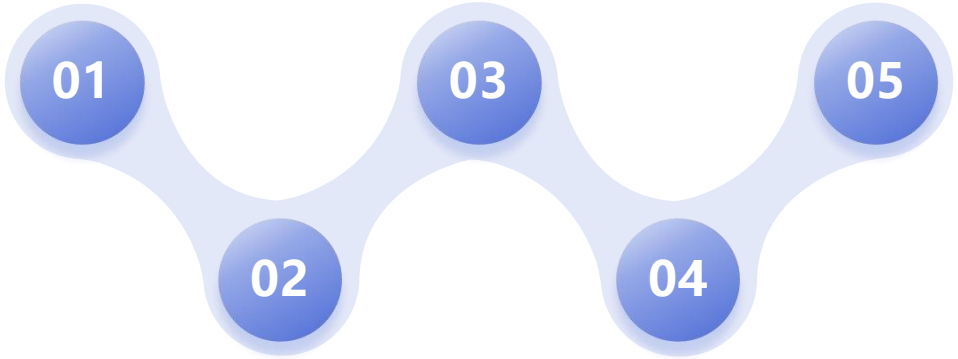
计算机先驱者冯·诺依曼曾构想病毒程序蓝图，20世纪70年代科幻小说构想首个计算机病毒。

国内病毒发展

80年代末，国内出现“黑色星期五”等病毒，因软件交流频繁且反病毒软件不普及而广泛流行。

病毒的特点与目的

病毒是精巧严谨的代码，需一定长度，非偶然形成。制作者目的多样，包括表现能力、报复、政治需求等。



第一例计算机病毒

1987年，美国发现首例计算机病毒巴基斯智囊病毒(Brian)，随后全球出现多种病毒。

病毒发展阶段

计算机病毒经历了多个发展阶段，包括DOS引导阶段、网络阶段等。

活动5 认识计算机病毒----计算机病毒的特征

01

传染性

病毒通过嵌入宿主程序实现自我复制和繁殖，通过移动存储设备和网络迅速传播。

02

衍生性

病毒变种多，通过分析病毒结构可衍生出新病毒，变种病毒后果可能更严重。

03

寄生性

病毒程序隐藏在正常程序中，难以区分，代码短小精悍，非常隐蔽。

04

破坏性

病毒对计算机系统具有破坏性，分为良性病毒和恶性病毒，恶性病毒破坏严重。

05

可触发性

病毒因特定事件或数值触发感染或破坏动作，如CIH病毒26日发作。

06

潜伏性

病毒进入系统后长期隐蔽，不立即发作，以提供足够时间繁殖扩散。

活动5 认识计算机病毒----计算机病毒的类型

01 单机环境下的传统病毒

文件病毒：寄生在可执行程序体内，激活后驻留内存并传染。

引导区病毒：感染主引导记录，系统启动时获得控制权并传播。

宏病毒：寄生于文档或模板宏中，打开文档时激活并驻留Normal模板。

混合型病毒：既感染可执行文件又感染磁盘引导记录。

02 现代环境下的网络病毒

蠕虫病毒：利用网络通信功能自我复制并传播，消耗资源，导致网络堵塞。

木马病毒：隐藏于正常程序中，非法入侵并监控用户计算机，窃取机密信息。

攻击型病毒：感染后对计算机软件或硬件进行攻击破坏。

活动5 认识计算机病毒----计算机病毒的破坏方式

破坏操作系统

病毒直接破坏操作系统的磁盘引导区、文件分区表、注册表，使计算机无法启动。

破坏数据和文件

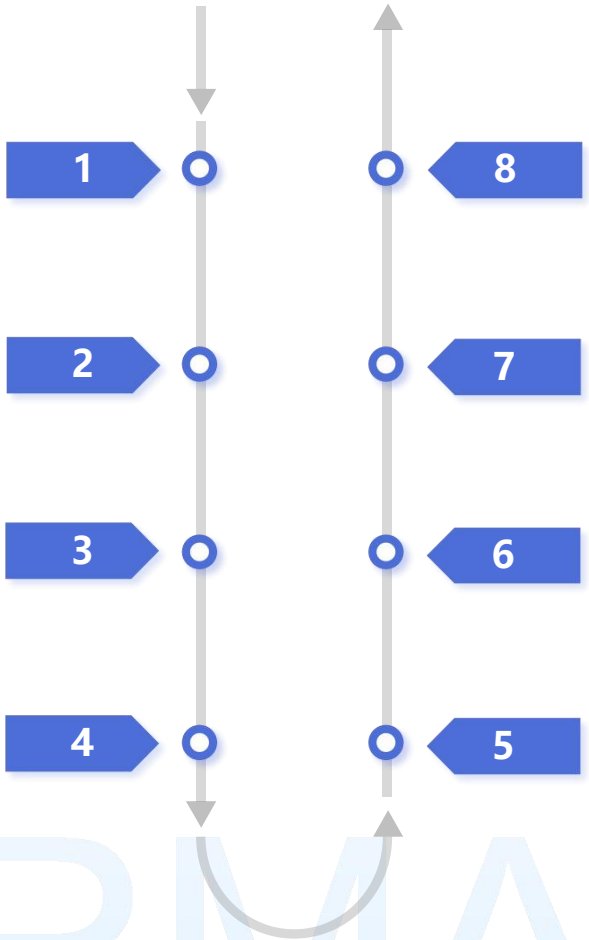
病毒改写或删除磁盘文件，导致数据永久丢失。

占用系统资源

病毒占用大量资源，使计算机运行缓慢或停止运行。

破坏网络

蠕虫病毒发送大量广播包，占用网络带宽，导致网络拥塞。



防治病毒的重要性

防治病毒是保障计算机系统安全的重要任务。

自动复制与感染

病毒自动复制、感染其他计算机，扰乱系统正常运行，危害社会。

扫描网络，开启后门

口令蠕虫病毒扫描网络，猜测口令，传送病毒，开启后门进行远程控制。

泄露信息

木马病毒泄露计算机信息，或向指定计算机传送数据。

活动5 认识计算机病毒----防范计算机病毒

病毒传播途径

计算机病毒的传播途径主要有两种：一是通过存储媒体载入计算机，比如U盘、移动硬盘、光盘等；另一种是在网络通信过程中，通过计算机与计算机之间的信息交换，造成病毒传播

病毒防范措施

备好无毒启动盘，避免用移动存储设备启动；定期备份重要资料；设置只读保护；不随意借入借出移动存储设备；重要部门计算机专机专用；使用新软件前杀毒；安装防病毒工具并定期升级；升级安全补丁；使用复杂密码；不随意下载软件或打开不明邮件附件。

病毒处理

发现病毒后迅速隔离受感染计算机，使用可靠查杀毒工具处理；硬盘资料受损时，使用灾后重建工具分析重建，不急于格式化。

活动5 认识计算机病毒----计算机病毒发作症状

- **响应迟钝**
- 计算机响应比平常迟钝，程序载入时间比平时长，病毒在系统启动时执行动作。
- **硬盘指示灯异常**
- 硬盘指示灯无缘无故亮起，无磁盘存取时，可能已感染病毒。
- **存储容量减少**
- 系统存储容量突然大量减少，病毒消耗系统资源。
- **磁盘空间减少**
- 磁盘可利用空间突然减少，病毒可能开始复制。

- **坏磁道增加**
- 坏磁道增加，病毒隐藏其中，杀毒软件难检测。
- **文件长度增加**
- 可执行文件长度增加，病毒增加程序长度。
- **死机现象增多**
- 计算机死机现象增多，病毒干扰系统正常运行。
- **文档异常**
- 文档消失、内容被改、名称、扩展名、日期或属性被更改，病毒攻击系统数据区、文件等。

活动5 认识计算机病毒----清除计算机病毒的方法

自动清除

一般用户使用杀毒软件清除病毒，具有防范和拦截功能，按菜单或联机帮助操作即可。

病毒防治策略

结合技术手段和管理机制，提高防范意识，制定规章制度，加强法制教育和职业道德教育，严惩非法活动，建立最佳的信息系统安全模式。

人工清除

利用工具软件打开被感染文件，找到并摘除病毒代码，复原文件，适合专业防病毒研究人员。

杀毒软件获取途径

购买或通过网络获取杀毒软件的免费试用版或演示版。

信息系统安全架构

物理安全 01

保护服务器、网络设备等硬件设施免受物理破坏或盗窃，包括数据中心的物理访问控制、环境监控等。

网络安全 02

包括防火墙、入侵检测/防御系统（IDS/IPS）、虚拟私有网络（VPN）等技术，确保数据在网络上传输时的安全性。

身份与访问管理 (IAM) 03

管理用户身份验证和授权的过程，使用密码策略、多因素认证 (MFA) 和权限管理等机制。

应用安全 04

在应用程序级别实施安全措施以防止漏洞被利用，包括代码审查、安全配置管理和使用安全开发实践。

数据安全与加密 05

保护敏感数据不被未授权访问或泄露，使用加密技术来保护静态数据和传输中的数据。

合规与审计 06

确保符合行业标准和法律法规要求，定期进行安全审计和风险评估。

活动6 认识信息系统安全架构

保护服务器、网络设备等硬件设施免受物理破坏或盗窃，包括数据中心的物理访问控制、环境监控等。

物理安全

管理用户身份验证和授权的过程，使用密码策略、多因素认证 (MFA) 和权限管理等机制。

身份与访问管理 (IAM)

保护敏感数据不被未授权访问或泄露，使用加密技术来保护静态数据和传输中的数据。

数据安全与加密

网络安全

包括防火墙、入侵检测/防御系统（IDS/IPS）、虚拟私有网络（VPN）等技术，确保数据在网络上传输时的安全性。

应用安全

在应用程序级别实施安全措施以防止漏洞被利用，包括代码审查、安全配置管理和使用安全开发实践。

活动6 认识信息系统安全架构

确保符合行业标准和法律法规要求，定期进行安全审计和风险评估。

合规与审计

实施安全政策和流程，使用安全信息和事件管理系统 (SIEM) 来监控和分析安全事件。

安全管理与监控

每个组织需根据自身需求和威胁定制安全策略，并随技术发展不断更新和改进安全架构。

安全架构的定制与更新

灾难恢复与业务连续性计划

制定应对突发事件的计划，确保关键业务功能可以持续运行，包括备份和恢复策略。

用户培训与意识提升

教育员工识别并避免潜在的安全威胁，提高整个组织的安全意识。

06

信息安全防范技术

任务6.5 培养信息安全素养

任务描述

信息安全防范技术的任务分析可以分为两个主要部分：预防和响应。预防阶段的任务包括风险评估、安全策略制定、身份与访问管理、网络防护、端点安全、数据保护、备份与恢复、以及安全培训与意识提升，这些任务的目标是通过建立强大的安全屏障来减少攻击的可能性和影响。

任务分析

01 **响应阶段任务**

安全监控与审计、应急响应计划、合规性管理，确保快速有效检测、响应、恢复，符合法规要求。

02 **信息安全防范体系**

通过预防与响应阶段任务，构建全面体系，保护信息资产免受威胁。

活动1 访问控制技术

访问控制概述

访问控制是实现既定安全策略的系统安全技术，管理资源访问请求，防止非授权访问。

访问控制技术的实施

通过用户注册和授权审查实施，需核对用户名和密码，监视访问操作，拒绝越权访问。

密码认证方式

存在于操作系统中，用户提交用户名和密码，系统核对后允许访问，但密码明文传送不安全。

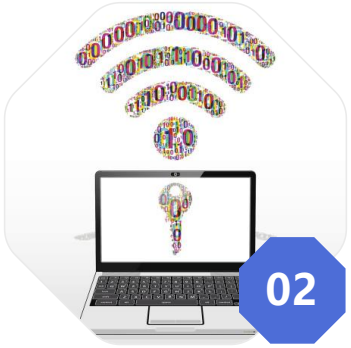
加密认证方式

弥补密码认证不足，使用请求与响应认证，双方持密钥K，系统生成随机数R，用户加密后传回，系统解密验证。

活动2 数据加密技术----基本思想

伪装信息

数据加密通过伪装信息，使非法介入者无法理解信息的真正含义。

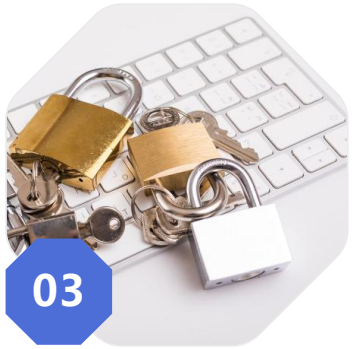


密文存储与传输

借助加密手段，信息以密文方式归档存储在计算机中或通过网络传输。

防止非法理解

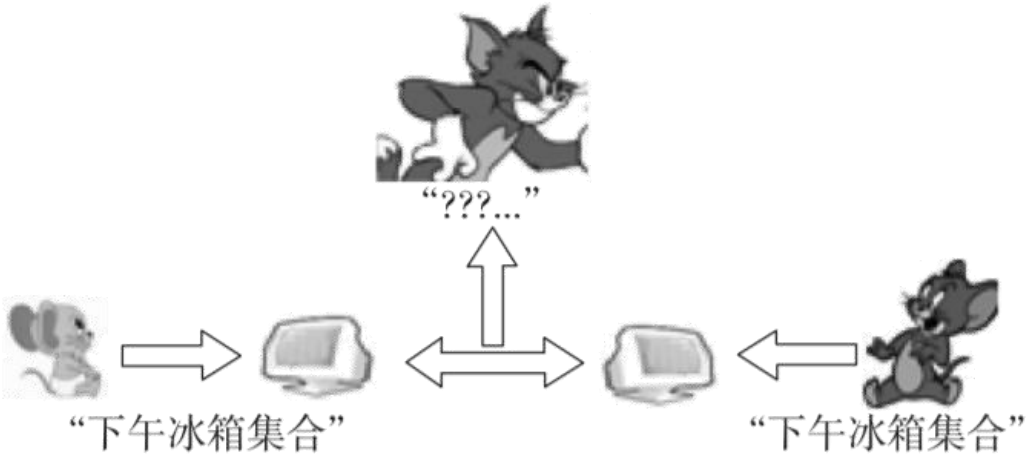
即使数据被非法截获或泄露，非授权者也无法理解数据的真正含义。



确保数据真实性

非授权者不能伪造有效密文篡改信息，确保数据的真实性。

活动2 数据加密技术----数据加密技术常用术语



- **明文**

  明文是需要传输的原文。

- **密文**

  密文是对原文加密后的信息。

- **密钥**

  密钥是控制加密结果的数字或字符串。

- **数据加密的重要性**

  数据加密是防止非法使用数据的最后一道防线。

活动2 数据加密技术----现代数据加密技术

加密算法与密钥

加密算法公开，密文可靠性在于不同密钥的不可破解性，保密性依赖于密钥。

密钥在加密解密中的作用

密钥与明文一起输入给加密算法，产生密文，破译密文实质是对密钥的破译。

加密算法评估与密钥破译

评估加密算法是评估其抵御密码被破解能力，破译密文是对密钥的破译。

破解技术与策略

破解技术基于穷举方法，提高安全性策略是使用优秀加密算法和更长密钥。

活动2 数据加密技术----对称加密技术

分组密码算法

- 分组密码算法将信息分成等长分组进行加密，如DES、IDEA、AES等。
- DES是首个分组密码算法，采用密钥逆序解密，有三重DES增强安全性。
- IDEA由中瑞学者提出，采用128位密钥加密64位数据，软硬件实现均易。
- AES由Rijndael算法入选，分组长度128位，密钥长度可变，安全高效。

序列密码算法

- 序列密码对明文每位用密钥流加密，相同明文加密后密文不同，难以破解。
- 序列密码易于硬件实现，加密速度快，广泛应用于军事领域，算法多不公开。

活动2 数据加密技术----非对称加密技术

- 在非对称加密技术中，采用了一对密钥：公开密钥(公钥)和私有密钥(私钥)。其中私有密钥由密钥所有人保存，公开密钥是公开的。在发送信息时，采用接收方公钥加密，则密文只有接收方的私钥才能解密还原成明文，这就确保了接收方的身份；另外，发送的信息采用发送方私钥加密，则密文使用对应的公钥可以解密还原成明文，这就确定了发送方的身份。这种机制通常用来提供不可否认性和数据完整性的服务。

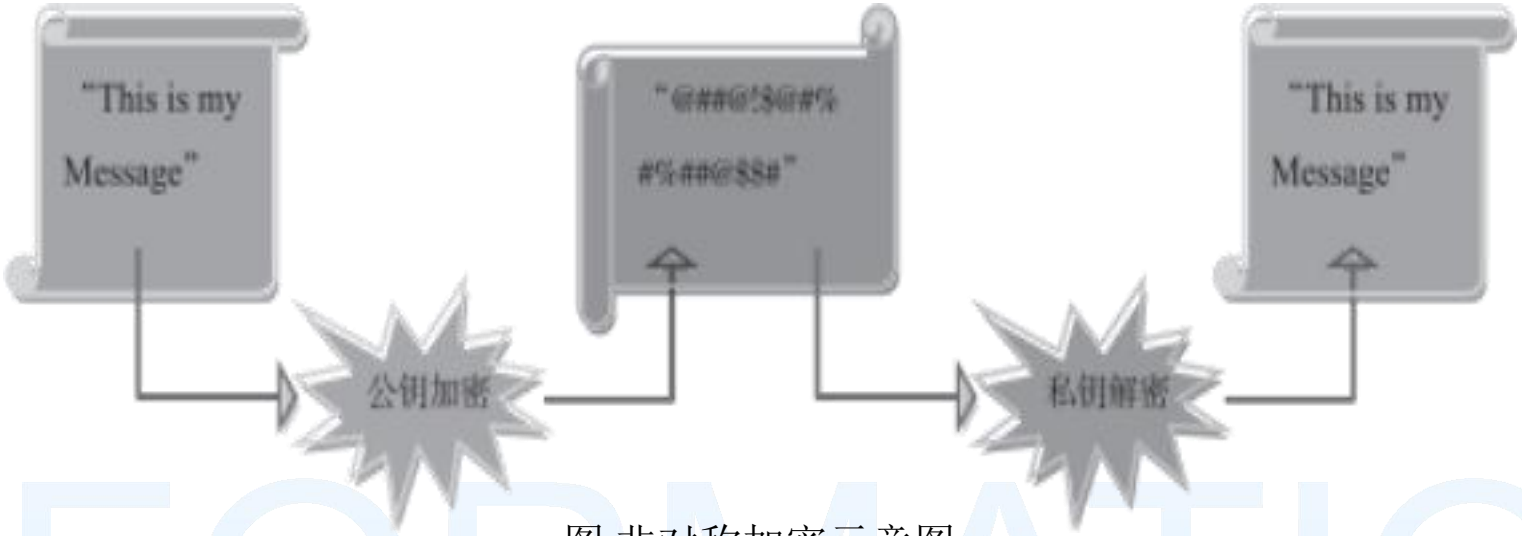


图 非对称加密示意图

活动2 数据加密技术----非对称加密技术

优点

非对称加密技术无需交换密钥，保障通信安全。

缺点

非对称加密技术的加、解密速度较慢，影响通信效率。

活动2 数据加密技术----非对称加密算法

Diffie - Hellman算法

Diffie - Hellman算法是第一个正式公布的公开密钥算法，由美国斯坦福大学学者迪菲和赫尔曼提出，可安全交换密钥。

RSA算法

RSA由Rivest、Shamir和Adleman在麻省理工学院开发，基于可逆模指数变换，素数越大安全性越高，广泛应用于数字签名和保密通信。

活动3 安全防御技术

01 网络信息安全威胁

网络中存在操作系统、通信协议及应用软件漏洞，数据在存储和传输中易泄露、窃取和篡改，威胁无处不在。

02 通信传输与存储攻击威胁

通信传输威胁、存储攻击威胁来自对信息的非法攻击，包括主动攻击与被动攻击。

03 主动攻击与防御技术

主动攻击通过伪造、篡改或中断等方法改变原始消息，常用技术有认证、访问控制与入侵检测等。

04 被动攻击与加密技术

被动攻击通过窃取方法非法获得信息，不改变消息，难以检测，采用加密技术对抗，保护信息安全。

05 安全防御技术分类

典型的安全防御技术包括认证、访问控制、入侵检测、加密技术等几大类。

活动3 安全防御技术----防火墙技术概述

防火墙是保护内部网络安全的技术，提供信息安全服务，实现网络和信息安全的重要基础设施。

位于被保护网络和外部网络之间，由硬件和软件组成，构成一道屏障。

过滤网络请求服务、隔离内网与外网的直接通信、拒绝非法访问等。

防火墙定义与功能

防火墙位置与构成

防火墙主要作用

活动3 安全防御技术----包过滤防火墙技术解析

包过滤防火墙示意图

01

包过滤技术概述

包过滤(PacketFilter)技术是所有防火墙中的核心功能，依据系统设置的过滤机制（ACL）在网络层对数据包进行选择。

02

访问控制列表配置

网络管理员编写ACL配置文件，置于边界路由器中，根据安全策略审查数据包IP报头，必要时审查TCP报头。

03

数据包处理流程

路由器接收数据包后，审查其报头与ACL规则匹配情况，允许则转发，拒绝则丢弃。

04

包过滤防火墙的优势

作为网络安全基本技术，包过滤防火墙实施几乎无额外费用，且不占用网络带宽。

活动3 安全防御技术----代理服务器防火墙概述

01

代理服务器技术

代理技术为应用级防火墙常用，需Internet访问权限主机作为代理服务器。

02

代理服务器作用

代理服务器为无权访问Internet的主机提供访问能力，增强网络灵活性。

03

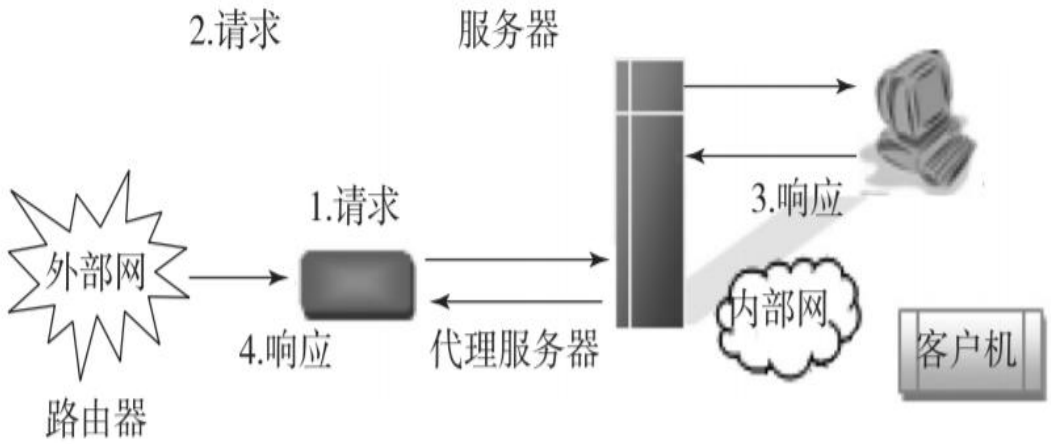
防火墙配置要求

内网主机需通过代理服务器与外网通信，增强安全性，代理服务器如真墙般防护。

04

通信安全机制

内外用户通信须经代理主机，增加攻击难度，确保通信安全。



代理服务器示意图

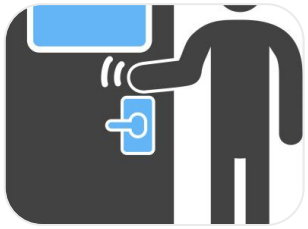
活动3 安全防御技术----身份识别技术概述

密码方式身份识别

采用5～8个数字、字母或特殊字符组成的字符串，广泛运用于各种场景。

标记方式身份识别

类似于个人持有的钥匙，用于启用个人电子设备，记录设备识别的个人信息。



新型身份识别技术

包括指纹识别、虹膜识别、人脸识别、区块链等，提高身份识别的安全性和便捷性。

活动3 安全防御技术----数字签名技术

01

数字签名概述

数字签名技术是公钥加密与数字摘要的综合运用，确保信息发送者身份及信息完整性。

02

签名过程

发送者用算法生成信息摘要，用私有密钥加密，与原文一同发送。接收者用公钥解密摘要，再生成摘要对比，验证信息完整性。

COLLECTING
DIGITAL SIGNATURES

活动4 安全攻击技术

01

黑客的定义与演变

黑客起源于20世纪50年代，初为褒义，指热爱解决难题、推动计算机技术发展的人。后演变为利用技术手段非法入侵计算机系统的人。

02

黑客的动机与行为

黑客认为信息应共享，反对垄断，因此将目标转向机密信息数据库。黑客行为包括截取数据、窃取情报、篡改文件、扰乱和破坏系统等。

03

黑客程序的特点

黑客程序是专门用于网络攻击的软件，能控制、盗取、破坏信息。它不是病毒，但可传播病毒，增强攻击能力。

活动4 安全攻击技术----网络攻击的一般步骤

01 信息收集

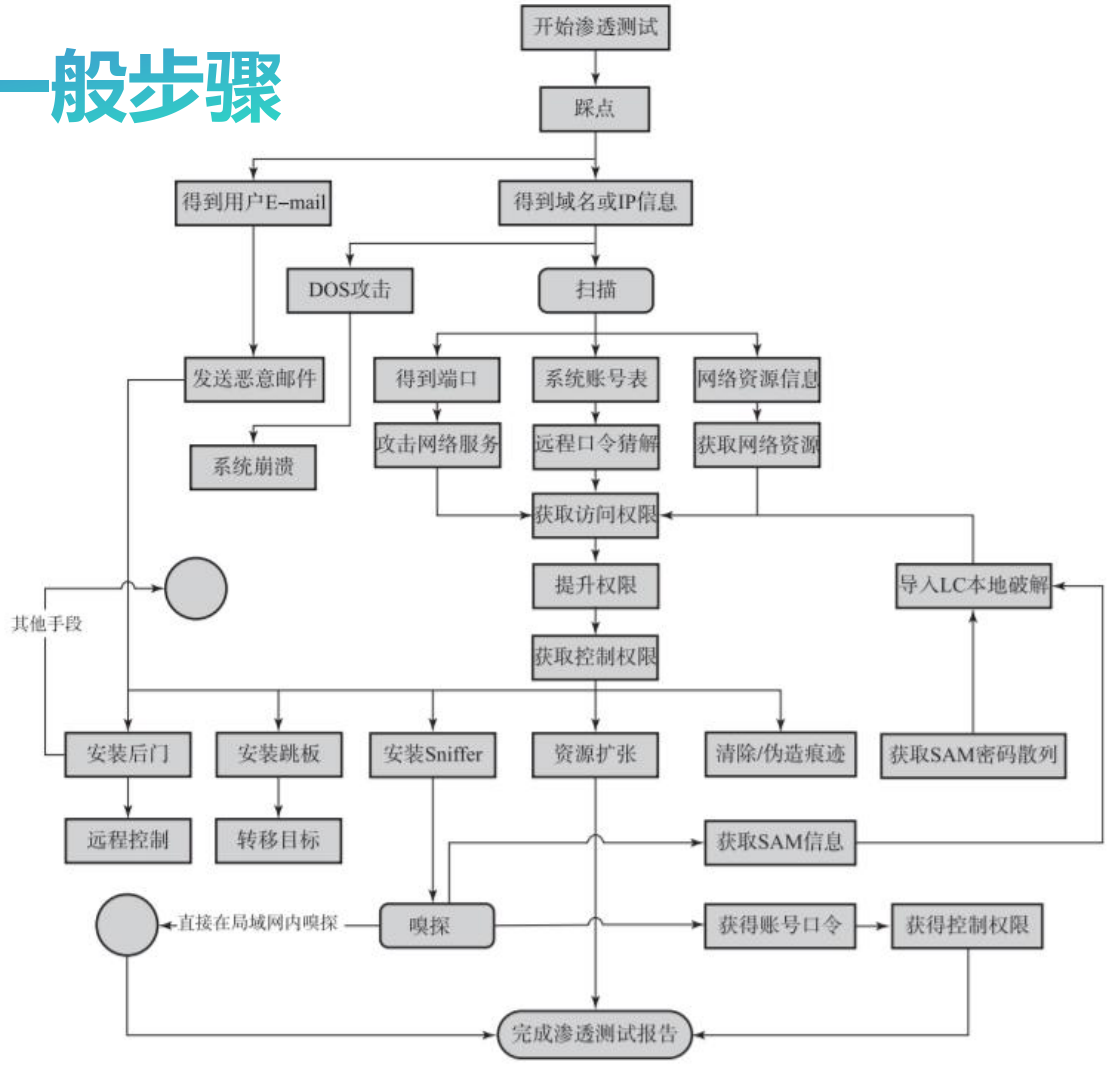
利用SNMP协议查看路由器路由表，TraceRoute程序获取网络数和路由数，Ping程序检测主机位置。

02 探测分析系统的安全弱点

使用TELNET、FTP等软件探测主机，使用ISS、SATAN等工具扫描网络，寻找安全漏洞，获取非法访问权。

03 实施攻击

毁坏入侵痕迹，建立新漏洞或后门，安装探测器软件，窥探系统活动，盗取敏感数据，毁坏重要数据。



网络攻击流程图

活动4 安全攻击技术----黑客的攻击方法

获取口令

通过网络监听、软件破解、暴力破解程序等方式获取用户口令，对局域网安全威胁巨大。

放置特洛伊木马程序

伪装成工具程序或游戏诱使用户打开，潜伏在计算机系统中，黑客可控制用户计算机。

篡改网页

黑客篡改用户访问的网页URL，使用户向黑客服务器发出请求，达到欺骗目的。

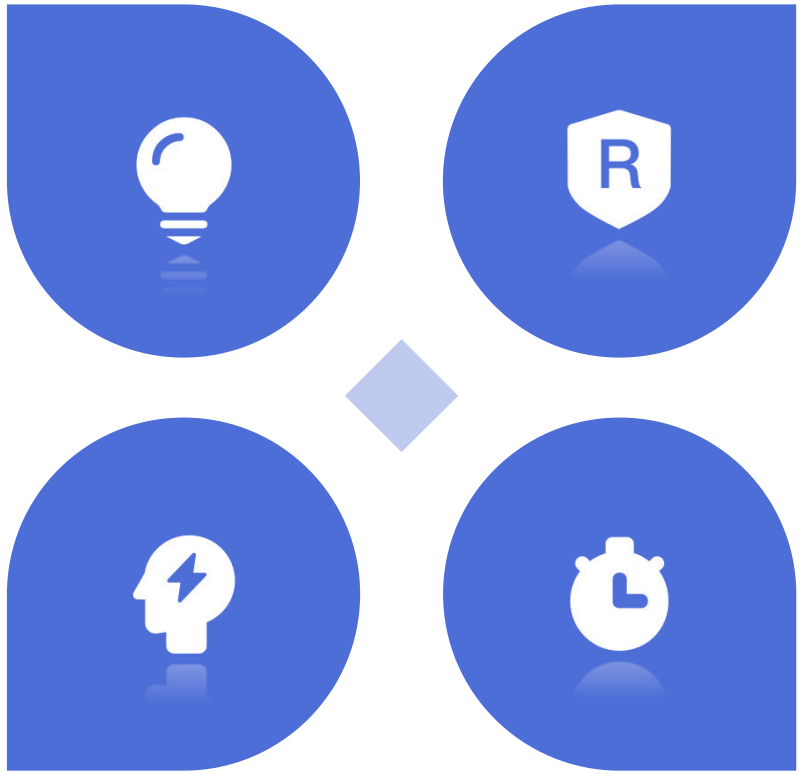
电子邮件攻击

电子邮件攻击包括邮件炸弹和电子邮件欺骗，前者发送大量垃圾邮件，后者伪装成系统管理员欺骗用户。

活动4 安全攻击技术----黑客攻击手段

通过一个节点攻击其他节点

黑客突破一台主机后，将其作为根据地，使用网络监听或IP欺骗等方法攻击其他主机。



网络监听

网络监听模式下，主机可接收本网段所有信息，未加密信息易被截取。

偷取特权

黑客利用特洛伊木马或缓冲区溢出程序，非法获得控制权或超级用户权限，危害极大。

系统漏洞

系统漏洞如缓冲区溢出，黑客可利用其改变程序执行流程，执行黑客程序。

活动4 安全攻击技术----黑客的防范

01 屏蔽可疑IP地址

发现可疑IP地址申请，通过防火墙屏蔽，但黑客可能更换IP或伪造IP。

02 过滤信息包

编写防火墙规则，丢弃攻击性信息包，但黑客可改变攻击形态或发送大量信息包。

03 修改系统协议

修改服务器协议，使漏洞扫描器失效，但需注意协议修改可能带来的其他问题。

04 经常升级系统版本

及时安装新版本或补丁程序，修补系统漏洞，预防黑客攻击。

05 及时备份重要数据

定期备份数据，确保系统受损时能迅速恢复，减少损失。

06 使用加密机制传输数据

选择破解困难的加密方法，如DES算法，保护数据传输安全。

活动5 常用第三方信息安全工具

- 在互联网时代，除了黑客和病毒威胁系统安全外，还存在木马、间谍软件等来自恶意软件的威胁，防病毒软件可以通过代码识别病毒或恶意软件，防火墙可以通过通信数据阻止非法访问，面对其他恶意软件的攻击，对强制修改注册表、系统文件、防火墙规则、禁用防病毒等恶意行为的恶意软件，可以使用安全防护软件来防范。
- 不过，应慎重选择第三方安全防护产品，多数安全防护产品会接管WindowsDefender反病毒软件，如360安全卫士、腾讯电脑管家、火绒安全等。部分还会接管WindowsDefender防火墙，如SymantecEndpointProtection。因此，在选择安全防护产品时，需要考虑防病毒软件和防火墙的替代方案，假如选择了360安全卫士做安全防护，还应安装360杀毒。有自带防病毒软件的安全防护产品，如火绒安全。有自带防病毒和防火墙的安全防护产品，如SymantecEndpointProtection。

活动5 常用第三方信息安全工具

01

防火墙

推荐品牌：思科、华为，有效抵御外部攻击，保障网络边界安全。

02

杀毒软件

推荐软件：360安全卫士、卡巴斯基，全面扫描，实时防护，确保系统安全。

03

加密软件

推荐软件：PGP、TrueCrypt，对敏感数据加密，保障数据传输与存储安全。

04

身份认证工具

推荐工具：Duo Security、Okta，多因素认证，增强账户安全，防止未授权访问。

05

安全审计工具

推荐工具：SolarWinds、LogRhythm，全面记录与分析系统活动，及时发现潜在威胁。

Cyber Securuty

INFORMATION

THANKS