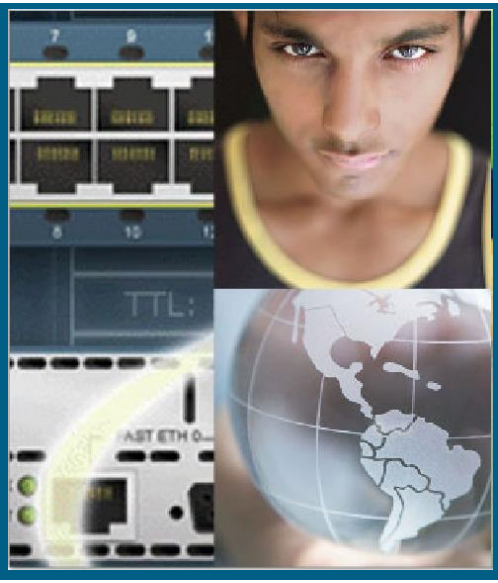
# 《无线网络应用》第五次课之一

4.03版在线教材 http://ebase.zju.edu.cn/ccna403
(Edge在IE模式下加载打开，要装Flash)



## 4. 03版 第8章
## 基本安全性

4. 03版 第8章 内容对应 7. 02版 以下章节

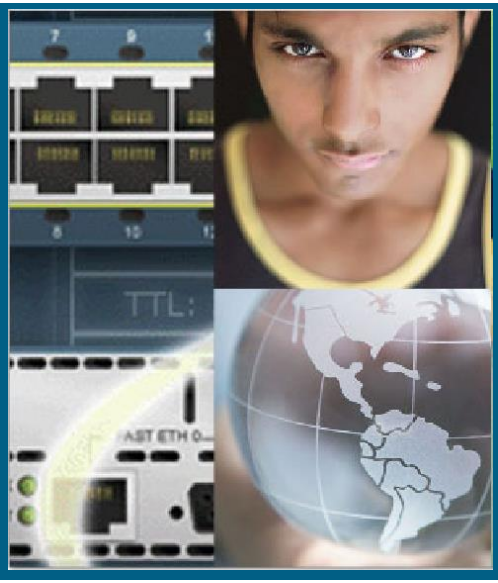
1. 6. 5节 网络安全、1. 8节 网络安全、模块16 网络安全基础知识

# 内容索引

# 学习目标

- 识别和描述各种网络威胁
- 识别各种攻击方式
- 描述安全规程和应用程序
- 描述防火墙的特点，
  以及如何应用防火墙来防范攻击

# 一、网络威胁



# 1、网络入侵风险

- 在计算机网络中，不速之客的入侵可能导致代价高昂的网络中断和工作成果的丢失。针对网络的攻击有时具有相当的破坏性，可能造成重要信息或资产的损坏或失窃，导致时间上和金钱上的损失。
- 入侵者可通过软件漏洞、硬件攻击甚至一些科技含量很低的方法（例如猜测某人的用户名和密码）来获得对网络的访问权。

✓ 通过修改软件或利用软件漏洞来获取网络访问权的入侵者通常被称为黑客(hacker)。

- 随着威胁、攻击和利用方式的不断发展，各种用于形容攻击参与者的术语层出不穷。最为常见的术语包括：

- 黑客(Hacker)——一般术语，历史上指计算机编程专家。最近，该术语常用于形容那些企图通过未授权方式恶意访问网络资源的人，带有贬义。

- 白帽客(White hat)—寻找系统或网络漏洞，然后向系统所有者报告以便其修复漏洞的个人。理论上他们并非滥用计算机系统。白帽客通常关心的是如何保护IT系统，而黑帽客则喜欢破坏IT系统安全。

- 黑帽客(Black hat)—为牟取个人利益或经济利益，利用计算机系统知识侵入非授权使用的系统或网络的群体。骇客即属于一种黑帽客。

- 骇客(Cracker)—用于更为准确地形容非法访问网络资源的恶意群体的术语。

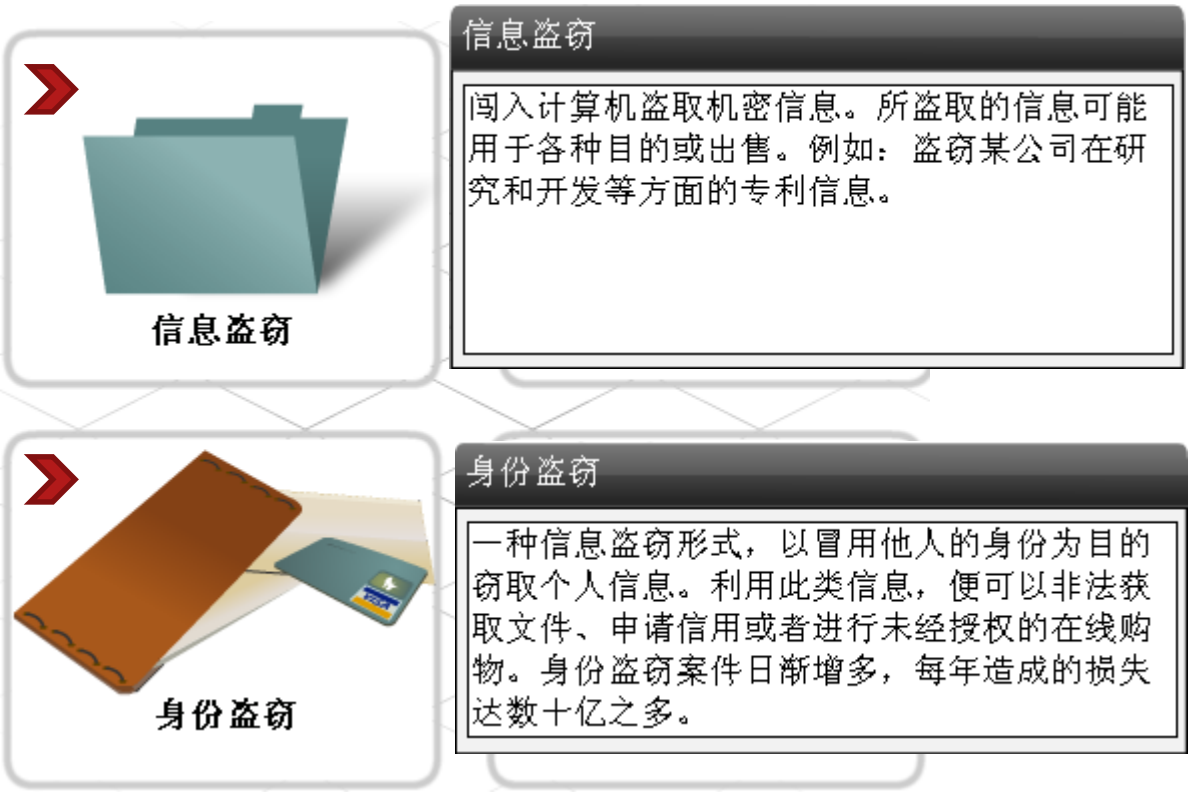
- 网络钓鱼者(Phisher)—指使用电子邮件或其它手段哄骗其他人提供敏感信息（如信用卡号码或密码）的个人。网络钓鱼者通常仿冒那些可以合法获取敏感信息的可信团体。

- 电话飞客(Phreaker)—指利用电话网络执行非法功能的个人。盗用电话网络的目的一般是侵入电话系统（通常通过付费电话）免费拨打长途电话。

- 垃圾邮件发送者(Spammer)—指发送大量未经请求的电子邮件消息的个人。垃圾邮件发送者通常利用病毒控制家用计算机，并利用它们发送大量消息。

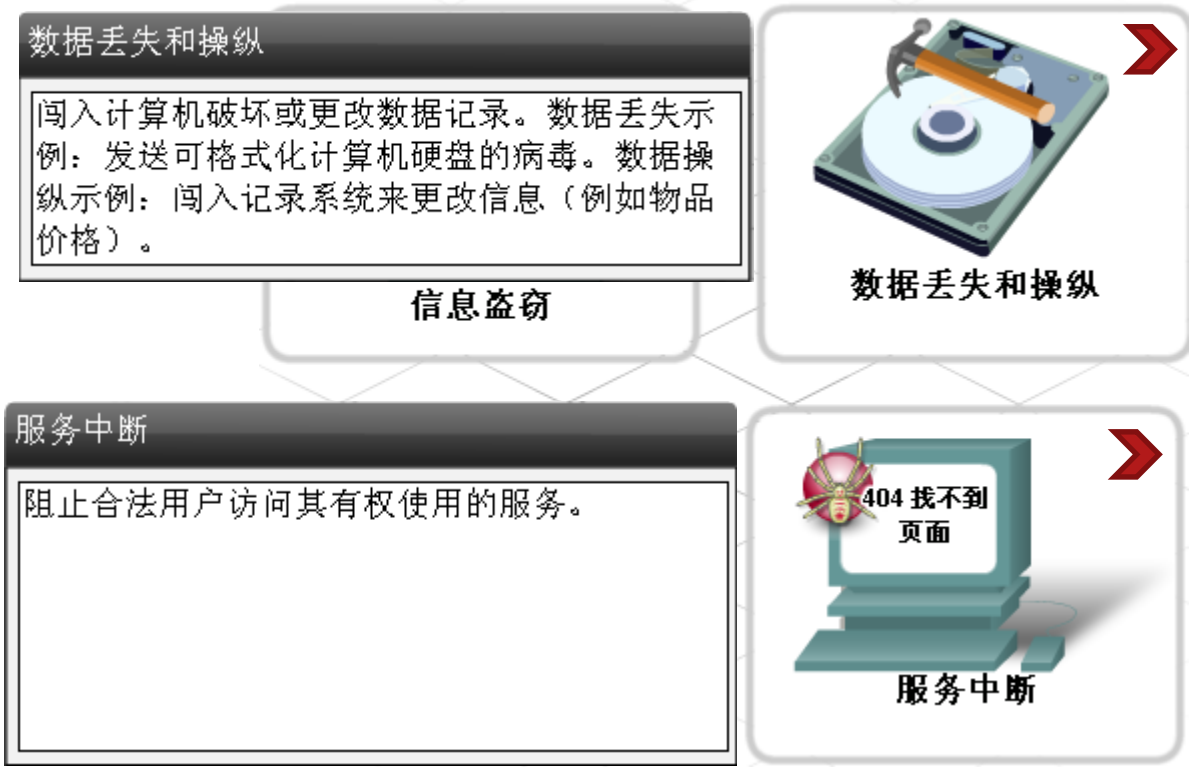
# 一旦黑客取得网络的访问权，就可能给网络带来以下四种威胁：

信息盗窃、身份盗窃、数据丢失和操纵、服务中断



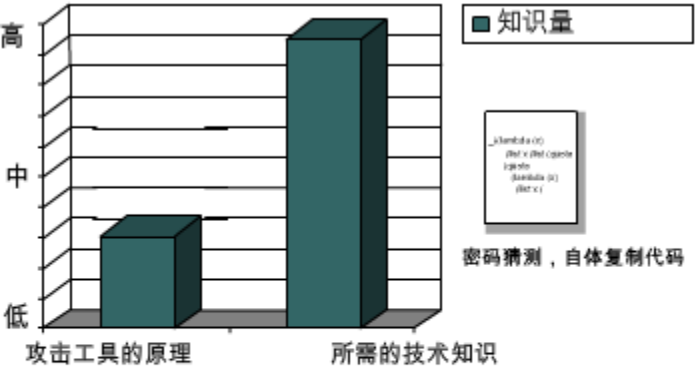
# 一旦黑客取得网络的访问权，就可能给网络带来以下四种威胁：

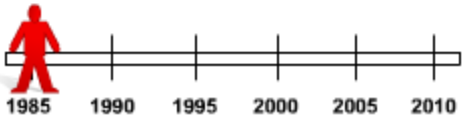
信息盗窃、身份盗窃、数据丢失和操纵、服务中断



- 近年来，网络攻击的工具和方法不断翻新。
- 以前，攻击者必须具备高深的计算机、编程和网络知识才能利用基本的工具进行简单的攻击。
- 随着时间的推移，攻击者的方法和工具不断改进，他们不再需要精深的知识即可进行攻击。这大大降低了对攻击者的门槛要求，许多以前无法参与计算机犯罪的人现在也有了这样的能力。

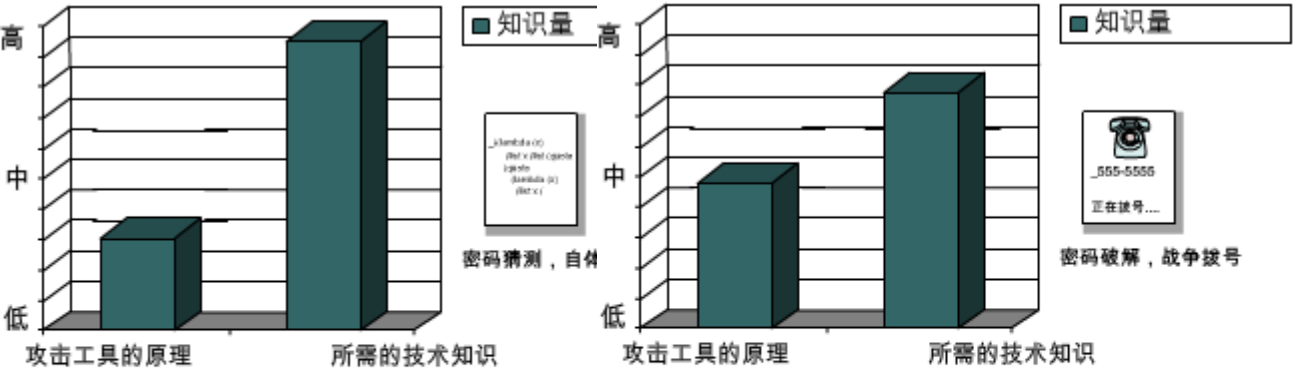
攻击工具的原理↑，所需的技术知识↓



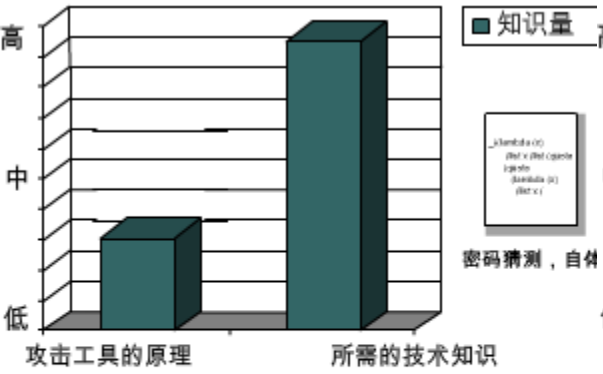
- 近年来，网络攻击的工具和方法不断翻新。
- 以前，攻击者必须具备高深的计算机、编程和网络知识才能利用基本的工具进行简单的攻击。
- 随着时间的推移，攻击者的方法和工具不断改进，他们不再需要精深的知识即可进行攻击。这大大降低了对攻击者的门槛要求，许多以前无法参与计算机犯罪的人现在也有了这样的能力。

攻击工具的原理↑，所需的技术知识↓



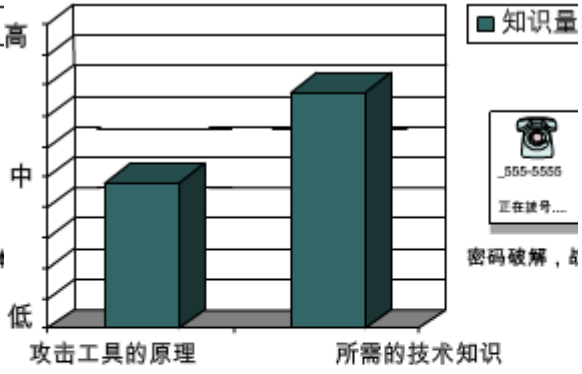

- 近年来，网络攻击的工具和方法不断翻新。
- 以前，攻击者必须具备高深的计算机、编程和网络知识才能利用基本的工具进行简单的攻击。
- 随着时间的推移，攻击者的方法和工具不断改进，他们不再需要精深的知识即可进行攻击。这大大降低了对攻击者的门槛要求，许多以前无法参与计算机犯罪的人现在也有了这样的能力。

攻击工具的原理↑，所需的技术知识↓





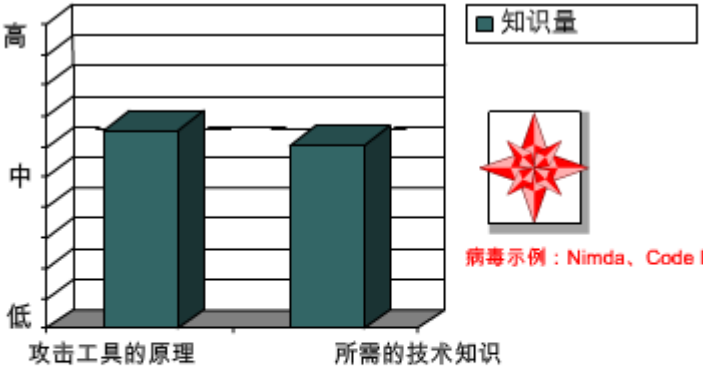

密码猜测，自





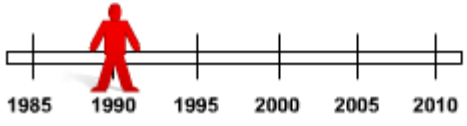


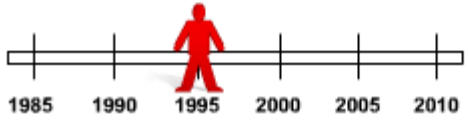
密码破解，





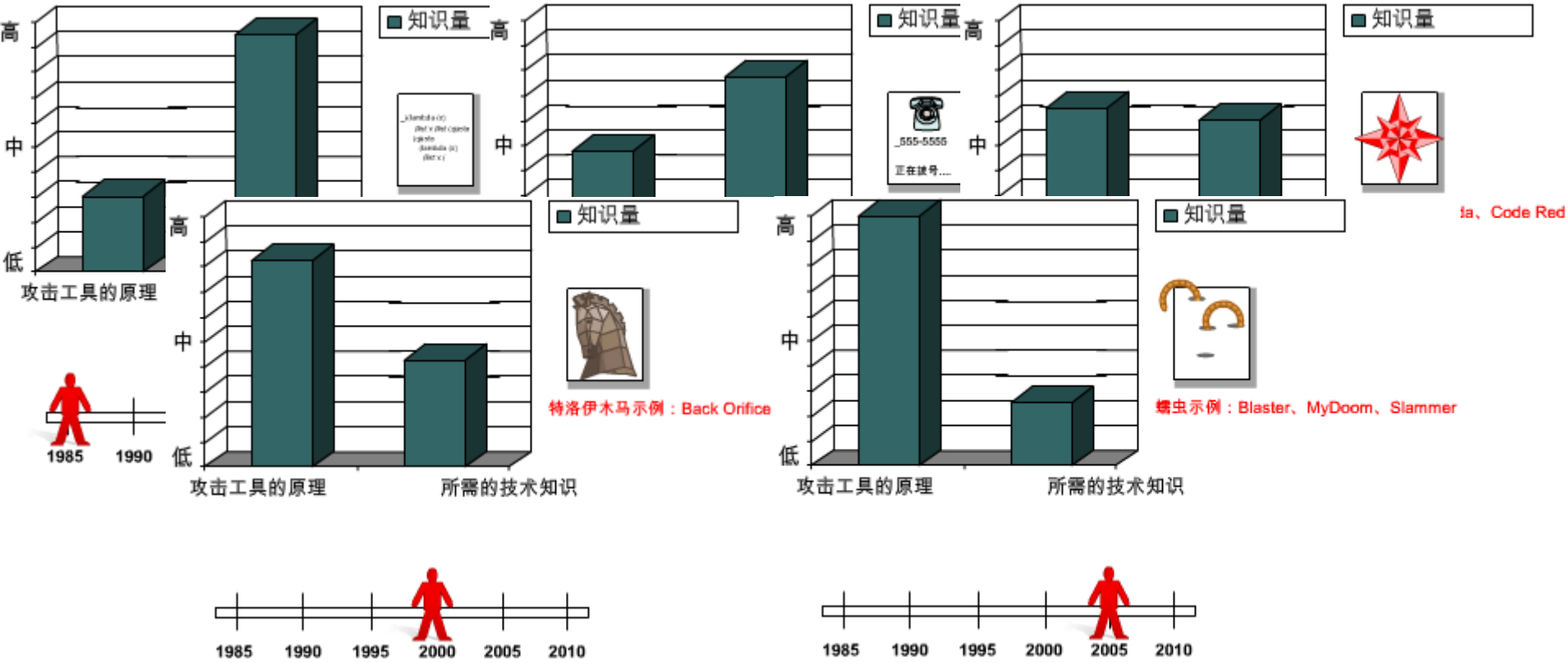

病毒示例：Nimda、Code Red

- 近年来，网络攻击的工具和方法不断翻新。
- 以前，攻击者必须具备高深的计算机、编程和网络知识才能利用基本的工具进行简单的攻击。
- 随着时间的推移，攻击者的方法和工具不断改进，他们不再需要精深的知识即可进行攻击。这大大降低了对攻击者的门槛要求，许多以前无法参与计算机犯罪的人现在也有了这样的能力。

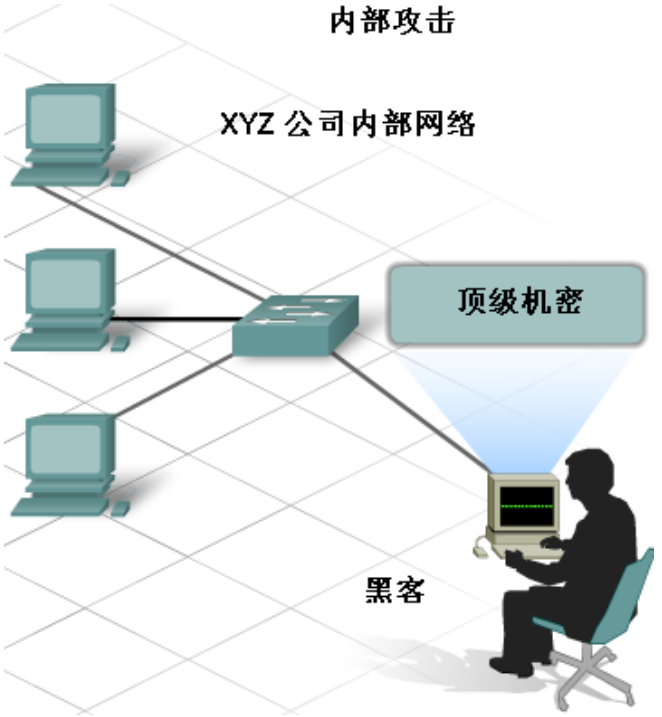
攻击工具的原理↑，所需的技术知识↓



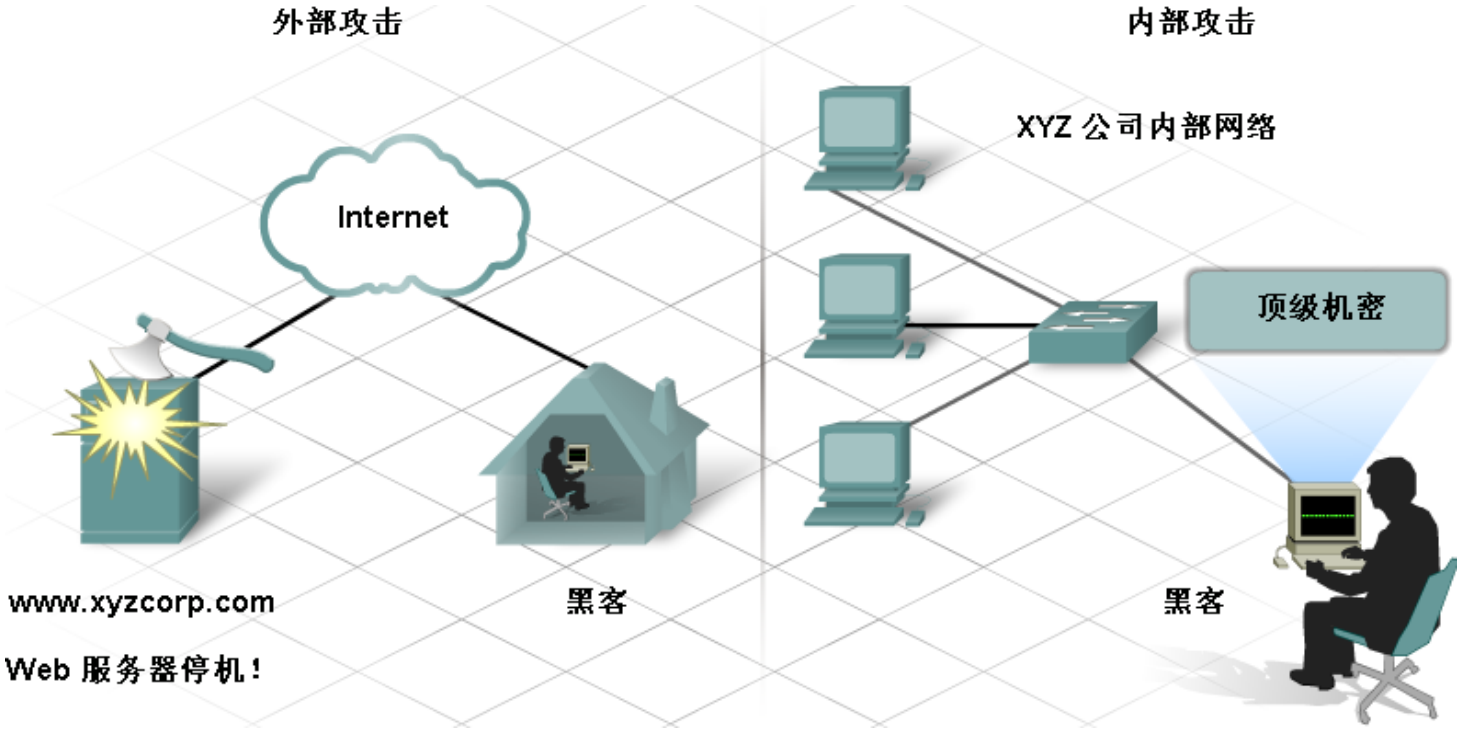
# 2、网络入侵的来源

- 网络入侵者造成的安全威胁可能来自网络内部和外部两个源头。
- 外部威胁是由组织外部活动的个人引起。他们没有访问组织内计算机系统或网络的权限。外部攻击者主要通过Internet、无线链接或拨号访问服务器进入网络。

- 内部威胁是由具有经过授权的用户账户的个人、或能够实际物理接触网络设备的人员导致的。内部攻击者了解内部政策和情况，清楚知道什么信息有价值且易受攻击，以及怎样获得这些信息。
- 并非所有内部攻击都是故意的。在某些情况下，一个受信任的员工在公司外部工作时可能会感染上病毒或蠕虫等安全威胁，在并不知情的情况下将它带到内部网络中，造成内部威胁。



- 许多公司都在防御外部攻击上花费了大量资源，但大多数威胁其实来自内部。
- 据FBI调查显示，在报告的安全入侵事件中，约有70%都是因内部访问和计算机系统账户使用不当造成的。



# 3、社会工程和网络钓鱼

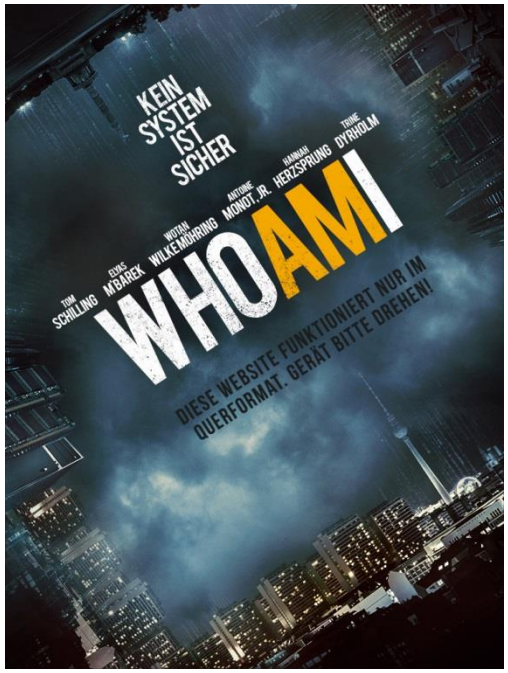
- 对于内外两个源头的入侵者而言，要想获得内部网络的访问权，最简单的一种方法就是：

  利用人类行为的弱点——容易轻信别人

- 常见方法之一：“社会工程”(Social Engineering)

- “社会工程”中最常用的三种“技术”是：假托、网络钓鱼、语音网络钓鱼


《我是谁：没有绝对安全的系统》（2014，德国、荷兰）



- 假托(Pretexting)是一种“社会工程”方式。攻击者会对受害人编造虚假情景，以使其泄漏信息或执行某种操作，从而使攻击者获得不当利益。

✓ 通常是通过电话联系攻击目标。

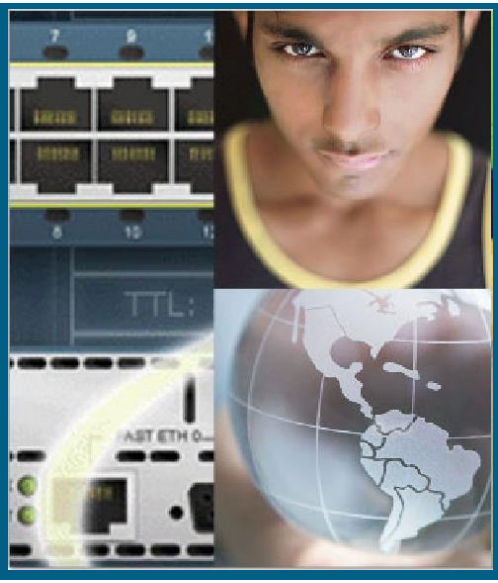
✓ 要使假托起作用，攻击者必须能够与攻击目标人员或受害人建立合理联系。为此，攻击者一般需要预先进行一些了解或研究。

- 例如，如果攻击者知道攻击目标的社会保险号码（美国的）或身份证号码（中国的），他们就会使用该信息来获取攻击目标的信任，那么攻击目标便很有可能进一步泄漏信息。

- 网络钓鱼(Phishing)是一种“社会工程”方式。网络钓鱼者将自己伪装成外部机构的合法人员。他们常通过电子邮件联系攻击目标个人（网络钓鱼受害者）。
- 网络钓鱼者可能会声称，为避免某些糟糕的后果，要求攻击目标提供确认信息（如密码或用户名）。

- 语音网络钓鱼(Vishing)/电话网络钓鱼(Phone Phishing)是一种使用IP语音(VoIP)的新式“社会工程”。
- 用户会收到一封语音邮件，邮件中指示他们拨打一个看上去像是正规电话银行服务的电话号码。随后，没有设防的用户拨打该号码时，通话会被窃贼截听。为了进行确认而通过电话输入的银行账号或密码便被攻击者窃取。

# 二、攻击方式



# 1、病毒、蠕虫和特洛伊木马

- 其它类型攻击，借助计算机软件的漏洞来执行。此类攻击技术包括：病毒、蠕虫、特洛伊木马。
- 所有这些都是侵入主机的恶意软件。它们会损坏系统、破坏数据及拒绝正常用户对网络、系统或服务的访问。它们还可将数据和个人详细信息从没有设防的PC用户转发到犯罪者手中。
- 在许多情况下，它们会自身复制，然后传播并感染连接到该网络的其它主机。

- 病毒是通过修改并附加到其它程序或文件上来运行和传播的一种程序。病毒无法自行启动，而需受到激活（人为启动其所附着的程序）。
- 有的病毒一旦激活，便会迅速自我复制并四处传播，但不会执行其它操作。这类病毒虽然很简单，但仍然非常危险，因为它们会迅速占用所有可用内存和CPU，导致系统死机。
- 编写得更为恶毒的病毒可能会删除或破坏特定类型的文件。如CIH病毒
- 病毒可通过电子邮件附件、下载的文件、即时消息或磁盘、光盘或USB设备（如U盘）传播。

- 蠕虫类似于病毒。与病毒不同的是，蠕虫无需将自身附加到其它程序或文件中。
- 蠕虫使用网络将自己的副本发送到任何连接的主机中。如冲击波、震荡波、熊猫烧香
- 蠕虫可独立运行并迅速传播，它无需激活或人类干预即可发作。自我传播的网络蠕虫所造成的影响可能比单个病毒更严重，而且可迅速造成Internet大面积感染。

- 特洛伊木马是一种没有自身复制能力的程序，以合法程序的面貌出现，实质上却是一种攻击工具。
- 特洛伊木马依赖于其合法无害的外表（一个实用工具或一个可爱的游戏）来欺骗和诱使受害人启动该程序。它的危害性可能相对较低，但也可能包含可损坏计算机硬盘内容的代码。如冰河、灰鸽子
- 特洛伊木马可为系统创建后门从而使黑客获得访问权。它一般由两部分组成：一是服务器程序，一是控制器程序。“中了木马”就是指被安装了木马的服务器程序。若你的电脑被安装了服务器程序，则拥有控制器程序的黑客就可以通过网络远程控制你的电脑了。

“特洛伊木马”的传说

- 特洛伊木马(Trojan Horse)的传说：

✓公元前12世纪，特洛伊(Troy)王子帕里斯访问希腊，诱走了王后海伦，希腊人因此远征特洛伊城。围攻九年后，到第十年，希腊将领奥德修斯献了一计，就是把一批勇士藏匿于一匹巨大的木马（“作战马神”）腹内，放在城外后，佯作退兵。特洛伊人以为敌兵已退，就把木马作为战利品搬入城中，饮酒狂欢。到午夜待全城军民皆睡去后，埋伏在木马中的勇士跳出来，打开城门，希腊将士一拥而入攻下了城池。

- 后来常用“特洛伊木马”这一典故，比喻在敌方营垒里埋下伏兵里应外合的活动。

(后门服务器)

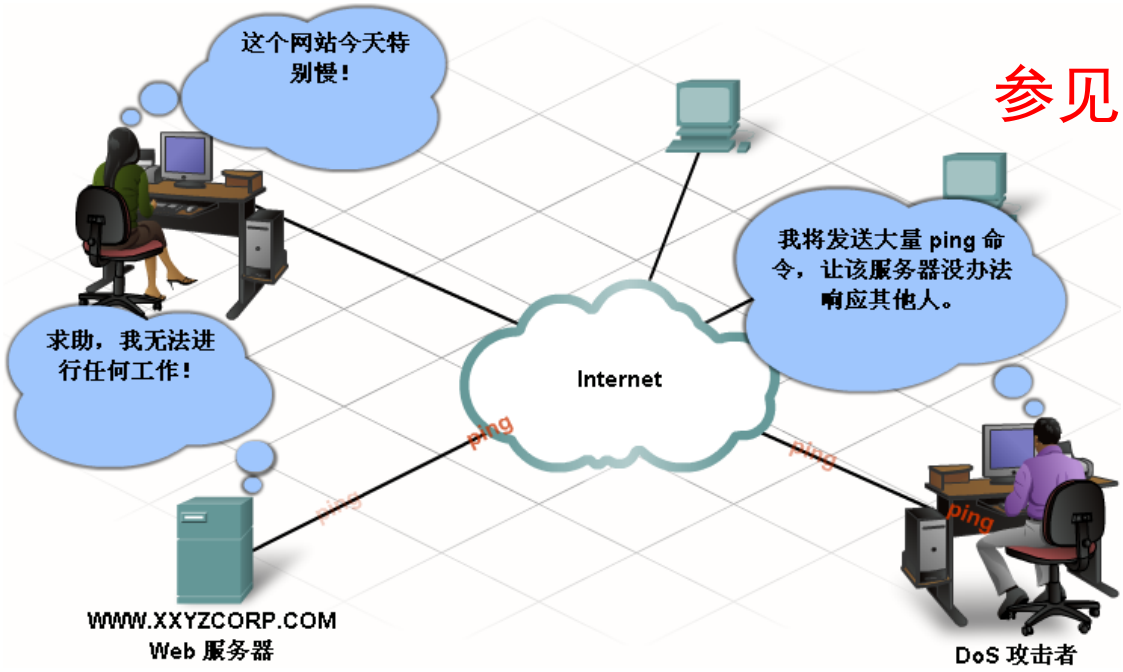
# 2、拒绝服务攻击

- 拒绝服务(DoS)攻击：DoS=Denial of Service
  是针对单个或一组计算机执行的一种侵略性攻击，目的是使服务器拒绝为特定用户提供服务。

- DoS攻击的意图：

✓ 使用通信量淹没服务器或网络（泛洪），阻止正常网络通信量通行。

✓ 中断客户端与服务器之间的连接，以阻止对服务的访问。




参见7.02版16.2.4节DoS攻击动画

- 两种常见的DoS攻击为：

1. SYN（并发）泛洪攻击：向服务器发送大量请求客户端连接的数据包，其中包含无效的源IP地址。服务器会因试图响应这些虚假请求而变得极为忙碌，导致无法响应合法请求。SYN泛洪攻击示意图
2. 死亡之Ping（即3D电影IPMovie - Warriors of the Net中的Ping of Death）：向设备发送超过IP协议所允许的最大大小（65,535字节）的数据包。这可导致接收设备系统崩溃。死亡之ping示意动画

DoS攻击的多种形式

| 资源过载 | 畸形数据 |
| --- | --- |
| 磁盘空间、带宽、缓冲区 | 数据包尺寸过大，例如死亡之 ping |
| Ping 泛洪，例如 smurf | 数据包重叠，例如 WinNuke |
| 数据包风暴，例如 UDP 炸弹和 fraggle | 无法处理的数据，例如 teardrop |

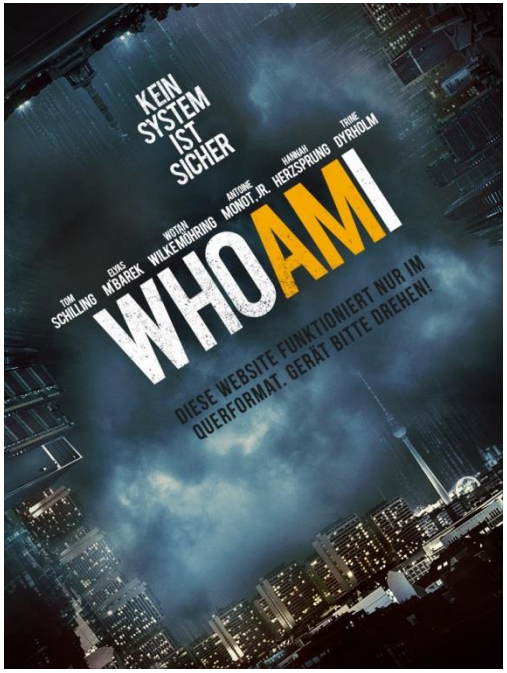
- 分布式拒绝服务(DDoS)攻击

✓ DDoS是更为狡猾、更具破坏性、运行规模更大的DoS攻击，通常会有成百上千个攻击点试图同时淹没目标。

✓ 攻击点可能是感染了DDoS代码的没有设防的计算机（俗称“肉鸡”或“僵尸计算机”），它们在被远程控制并被激活DDoS代码后对目标站点“群起而攻之”，最终导致其陷入瘫痪。

参见7.02版16.2.4节DDoS攻击动画

《我是谁：没有绝对安全的系统》（2014，德国、荷兰）



- 2014年8月，索尼的PSN及索尼在线娱乐网络都遭到DDoS攻击而瘫痪，同时遭受DDoS攻击的还有暴雪的战网及英雄联盟（非国服）的服务器。
- 2014年11月，索尼影业的网站被黑客入侵，攻击者“和平卫士（GOP）”将索尼的部分敏感信息公之于众。陷入黑客门的索尼极力挽回损失，据Recode报道，索尼用了**古老且激进**的**“以毒攻毒”**的方法进行回击：索尼动用了在亚洲的上百台电脑，使用了亚马逊网页服务（AWS），利用了位于新加坡和东京的服务器，对储存了偷窃数据的网站发起了DDoS攻击。
- 近几年来，伊朗和美国、以色列等国的网络战（DDoS）
- 2009年7月，韩国国防部等各大网站被黑（DDoS）
- 151130~151201，全球13个DNS根服务器中的每一个都遭到了每秒约500万次的DDoS攻击(bogus requests)

- **2016年10月22日**：一场始于美国东部的大规模互联网瘫痪席卷了全美，包括GitHub、HBO、Twitter、Reddit、PayPal、Netflix、Airbnb在内的许多知名网站均无法访问。此次断网事件持续了大约6个小时，经济损失近百亿美元。
- **造成本次大规模网络瘫痪的原因是Dyn公司的服务器遭到了DDoS攻击（每秒1TB甚至1.5TB流量的泛洪攻击）。**
  位于美国新罕布什尔州曼彻斯特市的Dyn是美国主要**DNS服务商**。
  **DNS遭到攻击，用户就无法用域名网址登陆网站。**

✓ Dyn首席策略师约克说：承载互联网基础设施核心的Dyn及其它公司成为越来越多DDoS的攻击目标，不仅遭受攻击数量和种类大增，而且攻击时长及遭受攻击的复杂性也都在增加。尤其是，随着智能产品的广泛使用，黑客可以在用户不知情的情况下，利用软件去控制成千上万的联网设备，如摄像头、家庭路由器等（成为“肉鸡”），通过海量的互联网流量去冲击一个目标。

- 在此次大规模断网事件中，黑客通过互联网控制了美国大量**网络摄像头**和**DVR录像机**，然后操纵这些“**肉鸡**”攻击多个知名网站。黑客们使用了一种**被称作“物联网破坏者”的Mirai病毒**来进行肉鸡搜索，这是一种通过互联网搜索物联网设备的病毒。当它扫描到一个物联网设备（如**网络摄像头**、**智能开关**等）后就尝试使用**默认密码**登录（Mirai自带约60个如图所示“**通用用户-密码组合**”），一旦登录成功，这台物联网设备就进入“**肉鸡**”名单，开始被黑客操控攻击其他网络设备。

- 约一百万台物联网设备（一说十多万台）参与此次DDoS攻击。参与本次DDoS攻击的网络摄像头及DVR设备，据说主要用了浙江大华公司 或 杭州雄迈科技 生产的摄像模组。

- 可见，今后能修改默认密码、安全性更高的物联网设备，将成为厂家、零售商和消费者的更好选择！

- 其实，网络安全研究员早已发出警告：万物互联IoE，物联网IoT，将会引发大量网络安全问题！而这场“史上最大的DDoS攻击”只是一个缩影！

| USER: | PASS: | USER: | PASS: |
|---|---|---|---|
| root | xc3511 | admin1 | password |
| root | vizxv | administrator | 1234 |
| root | admin | 666666 | 666666 |
| admin | admin | 888888 | 888888 |
| root | 888888 | ubnt | ubnt |
| root | xmhdipc | root | klv1234 |
| root | default | root | Zte521 |
| root | juantech | root | hi3518 |
| root | 123456 | root | jvbzd |
| root | 54321 | root | anko |
| support | support | root | zlxx. |
| root | (none) | root | 7ujMko0vizxv |
| admin | password | root | 7ujMko0admin |
| root | root | root | system |
| root | 12345 | root | ikwb |
| user | user | root | dreambox |
| admin | (none) | root | user |
| root | pass | root | realtek |
| admin | admin1234 | root | 00000000 |
| root | 1111 | admin | 1111111 |
| admin | smcadmin | admin | 1234 |
| admin | 1111 | admin | 12345 |
| root | 666666 | admin | 54321 |
| root | password | admin | 123456 |
| root | 1234 | admin | 7ujMko0admin |
| root | klv123 | admin | 1234 |
| Administrator | admin | admin | pass |
| service | service | admin | meinsm |
| supervisor | supervisor | tech | tech |
| guest | guest | | |
| guest | 12345 | | |

# DDoS攻击热点事件

第一次DoS攻击：1996年美国ISP公司Panix服务器
第一次DDoS攻击：1999年美国明尼苏达大学服务器

## 1.史上最大的DDoS网络攻击事件

- 2018年3月，知名代码托管网站GitHub遭遇DDoS网络攻击，1.35Tbps流量，攻击持续了8分钟以上。
- 2018年3月，针对一美国服务提供商客户DDoS攻击，峰值达1.7Tbps。
- 2020年2月，针对亚马逊Web服务AWS的DDoS攻击，2.3Tbps。
- 2020年10月，Google Cloud披露，他们在2017年9月防御了一次流量峰值高达2.54Tbps的DDoS攻击，其攻击目标是Google服务。
- 2023年8月，Google遭遇尖峰每秒3.98亿次的DDoS攻击，Cloudflare尖峰每秒2.01亿次，AWS尖峰每秒1.55亿次，都利用了0day漏洞HTTP/2 Rapid Reset。

## 2.海量移动设备沦为肉鸡事件

- 2019年4月，阿里云安全团队观察到数十起大规模应用层资源耗尽式DDoS攻击（应用层CC挑战黑洞攻击），这类攻击存在一些共同特征，发现这些攻击事件源于大量用户在手机上安装了某些伪装成正常应用的恶意App，该App在动态接收到攻击指令后便对目标网站发起攻击。
- 监测数据显示，近两个月已有五十余万台移动设备被用来当作黑客的攻击工具，达到PC肉鸡单次攻击源规模。不难看出，伪装成正常应用的恶意App已让海量移动设备成为新一代肉鸡，黑灰产在攻击手法上有进一步升级的趋势。

# 3、暴力攻击

- 暴力攻击

✓ 攻击者使用运行速度很快的计算机来尝试猜测密码或破解加密密钥。

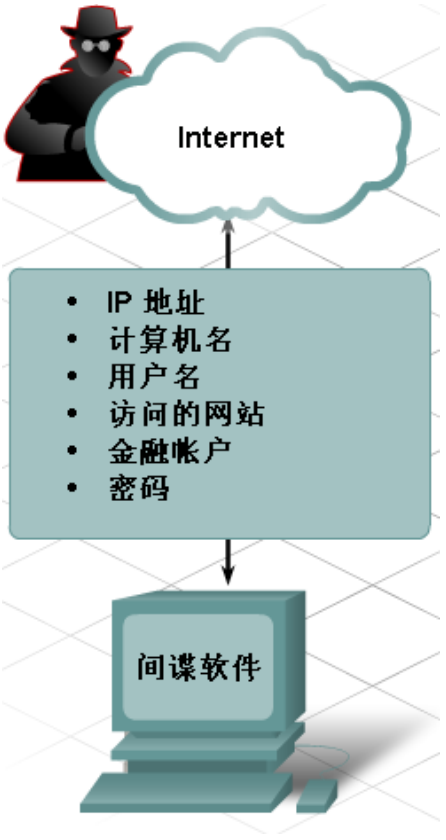
✓ 攻击者会在短时间内尝试大量可能的密码，来试图获取访问权限或破译密钥。

✓ 暴力攻击可引起针对特定资源的通信量过大或用户账户锁定（重试出错次数太多），导致合法用户被拒绝服务。

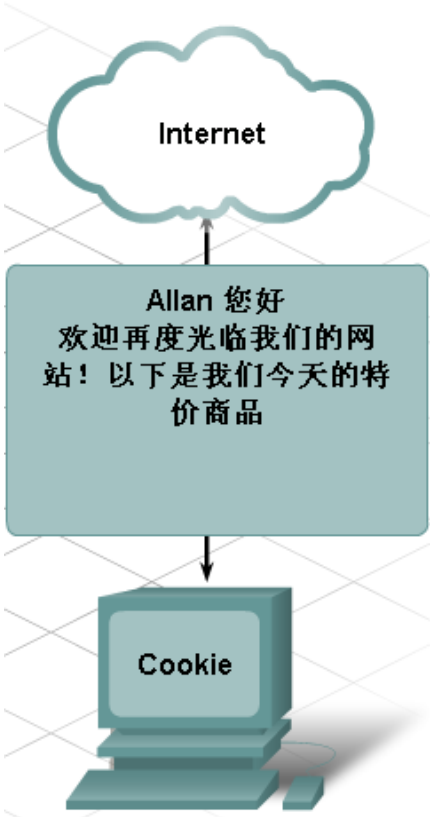
某学校安全保卫处提醒：
防范电信网络诈骗的紧急止付方法：（与暴力攻击异曲同工）
1、到银行柜台“故意多次输错诈骗账号密码”直至该账号被锁定。
2、拨打诈骗账号所属银行客服电话，选择银行卡挂失，输入诈骗者卡号后故意输错支付密码3-5次，直至听到“此账号密码多次输入错误，已暂停使用”等语音提示。
3、登录银行网站，多次将诈骗账户网银密码输错，将网银锁定。

# 4、间谍软件、跟踪Cookie、广告软件和弹出广告

- 许多网络威胁的目的是收集用户的相关信息以用于广告。尽管它们可能不会损坏计算机，但仍会侵犯隐私，而且非常招人反感。
- 间谍软件Spyware是一种程序，用于在未得到用户认可或用户不知情的情况下从计算机中收集个人信息。然后，这些个人信息会发送至Internet上的广告商或第三方，其中可能包含密码和账号等隐私信息。
- 间谍软件通常是在下载文件、安装其它程序或点击网页广告时暗中安装的。它会降低计算机速度，更改计算机内部设置，导致更多漏洞暴露给其它网络威胁。此外，间谍软件也难以删除（“流氓软件”）。



- 跟踪Cookie是间谍软件的一种形式，但也有一些Cookie起到积极的作用。它用于在Internet用户访问网站时记录用户的访问信息。由于它允许个性化定制及其它一些节省时间的方法，所以可能相当有用并受人欢迎。现在许多网站都要求用户启用浏览器的Cookie功能后才能正常访问。




- 广告软件Adware是另一种形式的间谍软件，它通过用户访问的网站来收集用户信息，这些信息之后会被利用来进行针对性的广告宣传。广告软件一般是作为用户使用“免费”产品或软件的交换条件而安装的，会影响网上冲浪的速度，一般也难以卸载。

- 弹出广告和背投广告是用户在浏览网站时显示的附加广告宣传窗口。
- 与广告软件不同，弹出广告和背投广告并不收集关于用户的信息，而且通常只与所访问的网站关联。

✓ 弹出广告在当前浏览器窗口前端打开（有焦点）。

✓ 背投广告在当前浏览器窗口后端打开（无焦点）。

# 5、垃圾邮件

参见4.03版教材动画8.2.4

- 通过Internet大量散发邮件进行营销或其它非法宣传的方法称为垃圾邮件(Spam)。垃圾邮件已成为非常严重的网络威胁，可导致ISP及电子邮件服务器不堪重负而过载。垃圾邮件通常是利用未受安全保护并开放转发功能的电子邮件服务器来转发的。
- 垃圾邮件不仅惹人讨厌，有时还携带病毒和其它安全威胁，可能被植入病毒或特洛伊木马代码从而远程控制用户主机，让受控主机在用户毫不知情的情况下发送垃圾邮件（受此形式感染的计算机称为垃圾邮件工厂spam mill）。
- 与时俱进的垃圾信息：今日头条AI作品、短彩信、微博、微信、App等都成了垃圾信息传播的新载体。

浙江大学信息技术中心微信公众号：
网络安全宣传周230911~230917
https://mp.weixin.qq.com/s/ZCKSFEi0MV3A-x1oXj_OKw


浙江大学微信公众号：网络安全宣传周来了！220905~220911

https://mp.weixin.qq.com/s/DDNkKnOIjzCzIi59Nc7z1g

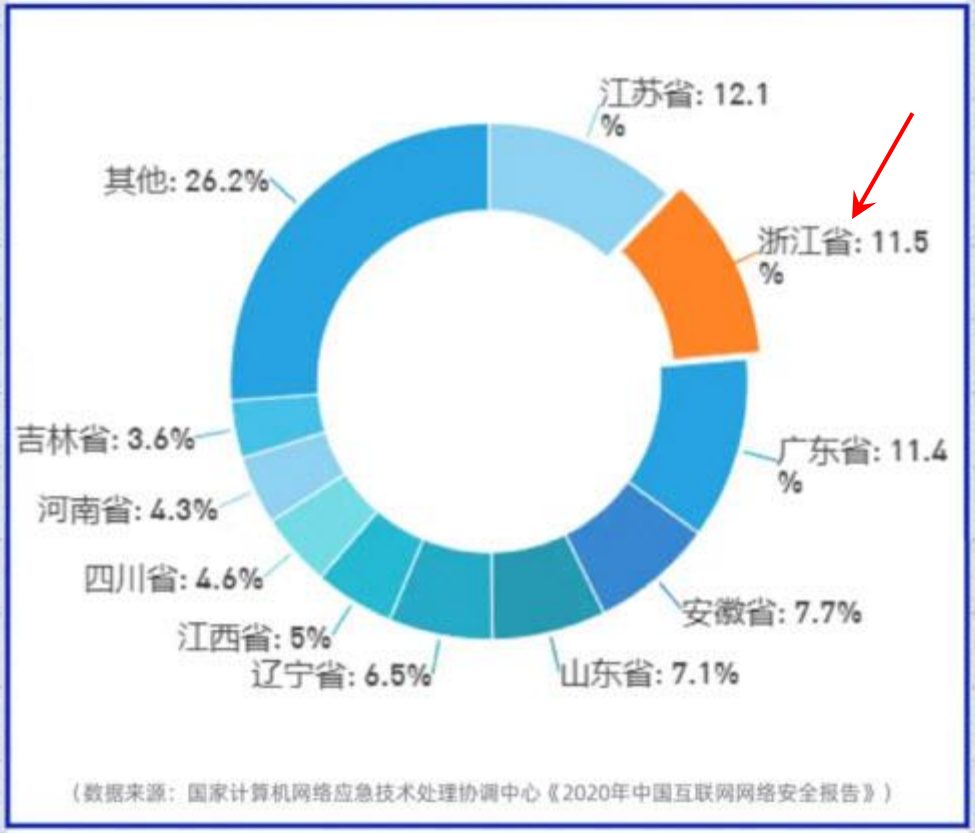
浙江大学微信公众号：纯干货科普！网络安全版扫“黑”风暴来了！
https://mp.weixin.qq.com/s/GbvPRcaH46ooLzRyvjmmfw

## 就全国而言

- 2020年利用安全漏洞针对境内主机远程攻击行为日均超过2176.4万次，捕获勒索病毒软件78.1万余个。

## 就浙江省而言

2020年我国境内感染计算机恶意程序主机地区分布图中浙江省受到的恶意程序攻击占全国的11.5%位居全国第二。




（数据来源：国家计算机网络应急技术处理协调中心《2020年中国互联网网络安全报告》）

也就是说，每10台感染恶意程序的计算机主机，

就有1.15台是浙江人的。

## 就我校而言

2020年“网上浙大”在不知不觉中

为学校防御770万次网络攻击，

防止了1.27亿次信息泄露。

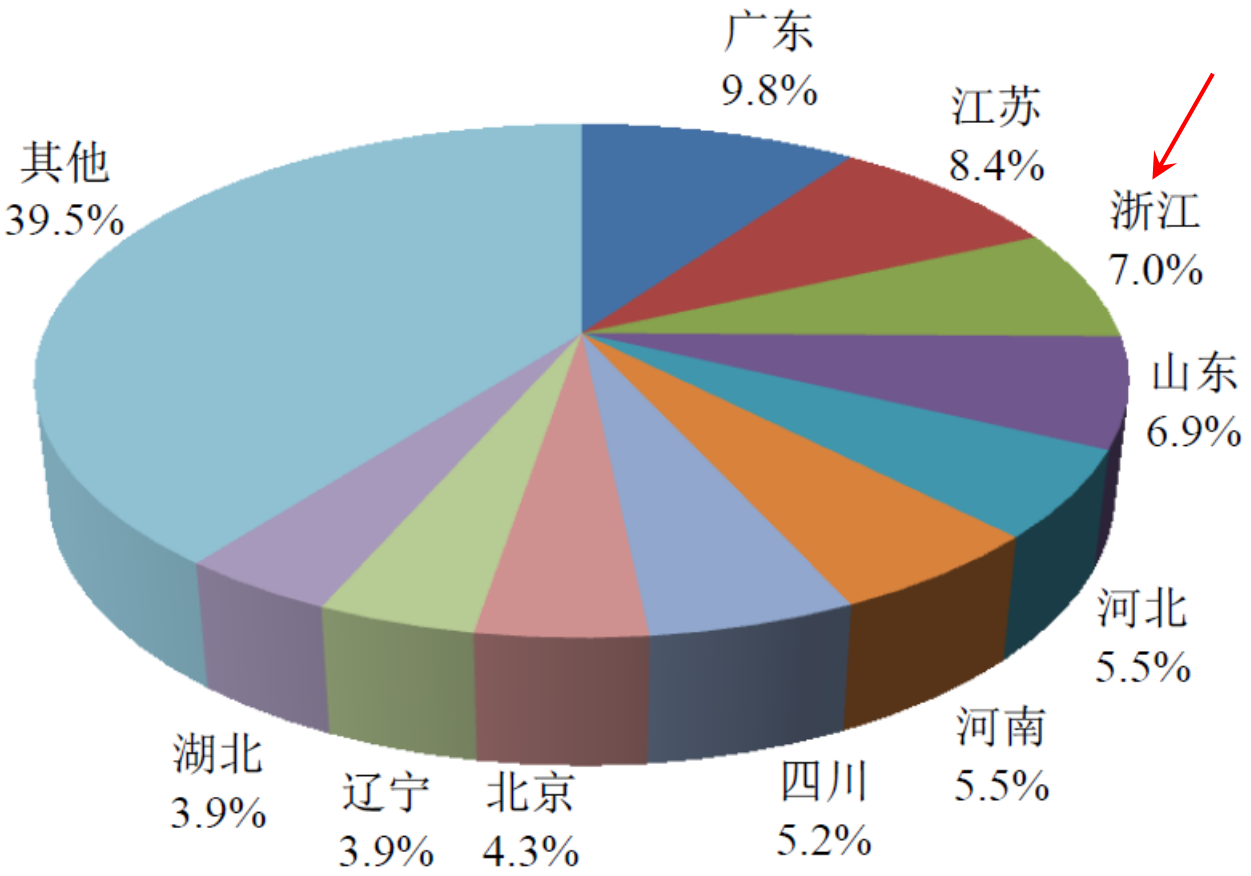



图 2 我国受恶意程序攻击的 IP 分布情况

《2021年上半年我国互联网网络安全监测数据分析报告》
国家计算机网络应急技术处理协调中心，2021年7月

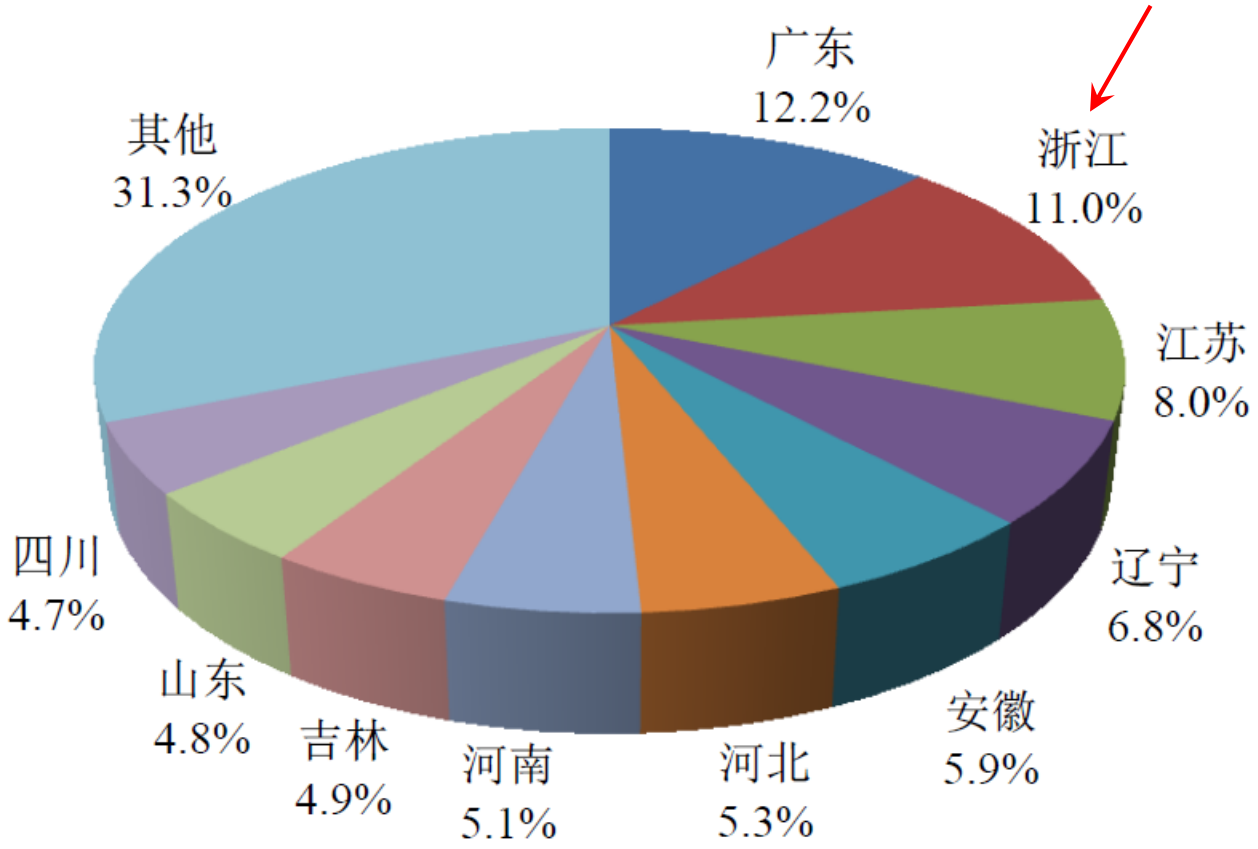



图 5 我国境内感染计算机恶意程序主机数量按地区分布

**《2021年上半年我国互联网网络安全监测数据分析报告》**
**国家计算机网络应急技术处理协调中心，2021年7月**

# 境内目标遭大流量DDoS攻击情况

- CNCERT监测发现，境内目标遭受峰值流量超过1Gbps的大流量攻击事件的主要攻击方式为TCP SYN Flood、UDP Flood、NTP Amplification、DNS Amplification、TCP ACK Flood、和SSDP Amplification，这6种攻击的事件占比达到96.1%;
- **攻击目标**主要位于**浙江省**、山东省、江苏省、广东省、北京市、福建省、上海市等地区，这7个地区的事件占比达到81.7%;
- 1月份是上半年攻击最高峰，攻击较为活跃;
- **攻击时长不超过30分钟的攻击事件高达96.6%**，比例进一步上升，表明攻击者越来越倾向于利用大流量攻击瞬间打瘫攻击目标。

《2021年上半年我国互联网网络安全监测数据分析报告》
国家计算机网络应急技术处理协调中心，2021年7月

# 被用于进行DDoS攻击的网络资源活跃情况

- CNCERT通过对境内目标遭大流量DDoS攻击事件持续分析溯源，发布《我国DDoS攻击资源季度分析报告》，定期公布控制端、被控端、反射服务器、伪造流量来源路由器等被用于进行DDoS攻击的网络资源情况，并进一步协调各单位处置。

- 累计监测发现用于**发起DDoS攻击**的**活跃控制端**1455台，其中位于境外的占比97.1%，主要来自美国、德国和荷兰等；

- **活跃肉鸡**71万余台，其中位于境内的占比92.7%，主要来自广东省、辽宁省、江苏省、福建省、**浙江省**等；

- **反射攻击服务器**约395万余台，其中位于境内的占比80.7%，主要来自**浙江省**、广东省、辽宁省、吉林省、四川省等。

反射攻击：攻击者向服务器发送大量请求，每个请求都以受害者IP地址为源地址。服务器对这些请求作出回应，向受害者发送大量回应。可能导致受害者网络连接过载，破坏他们对网络资源的访问。

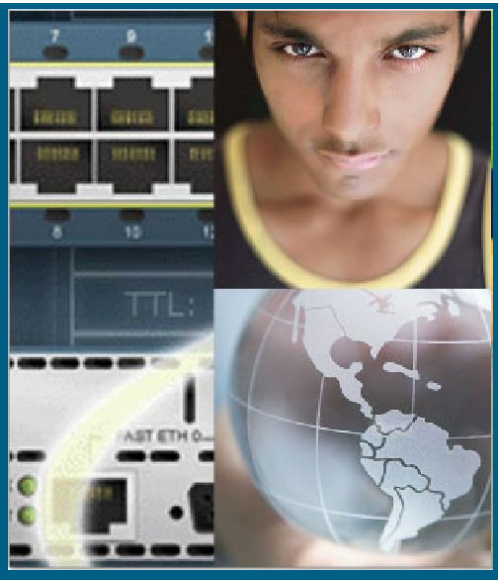
**《2021年上半年我国互联网网络安全监测数据分析报告》**
**国家计算机网络应急技术处理协调中心，2021年7月**

# 2023年网络安全态势研判分析

- **IPv6攻击较去年增长20.34%；全年全网网络层的DDoS攻击次数2.51亿次，攻击带宽峰值1,719.81Gbps，CC攻击5,513亿次，**受DDoS攻击影响最严重的是游戏行业，国内受DDoS攻击次数最多的是广东；新收录互联网安全漏洞5,252个；深信服拦截恶意程序210.30亿次，挖矿第1，木马第2；移动互联网安全态势稳定，新捕获样本数总量呈稳步增长趋势；物联网态势仍严峻，攻击者重点针对消费级IoT设备及特定企业的存在漏洞的IoT设备进行攻击；工业互联网、区块链安全态势相对稳定；**本年新增1,045个车联网漏洞**，其中高危漏洞626个，攻击态势仍严峻；**本年累计捕获超过1,200起针对我国的APT攻击活动**（高级长期威胁，Advanced Persistent Threat）。

《2023年网络安全态势研判分析年度综合报告》
中国网络空间安全协会，2024年1月

# 三、安全策略



# 1、常用安全措施

- 安全风险无法彻底消除或预防。但有效的风险管理和评估可显著减少现有的安全风险。
- **要将风险降至最低，必须认识到一点：没有任何一件产品可为组织提供绝对的安全保护。要获得真正的网络安全，需要结合应用多种产品和服务、制定彻底的安全策略严格实施。**
- **安全策略**是对规则的正式声明，用户在访问技术和信息资产时必须遵守这些规则。

（简单了解）

- **安全策略**应包含以下内容：
  - ✓标识和身份验证策略
  - ✓密码策略（例如思科网院官网netacad的密码）
  - ✓合理使用规定
  - ✓远程访问策略
  - ✓网络维护程序
  - ✓事件处理步骤

参见4.03版教材动画8.3.1.1

- 安全策略通过安全规程实施。这些规程定义了主机和网络设备的配置、登录、审计和维护过程。其中包括使用预防性措施来降低风险，及采用主动措施来处理已知的安全威胁。

- 可保护网络安全的一些安全工具和应用程序有：
  - ✓软件补丁和更新
  - ✓病毒防护工具
  - ✓间谍软件防护工具
  - ✓垃圾邮件拦截器
  - ✓弹出广告拦截器
  - ✓防火墙


参见4.03版教材动画8.3.1.2

# 2、更新和补丁

- 黑客用来获取主机和/或网络访问权的最常见方法之一是利用软件漏洞，因而及时对软件应用程序应用最新的安全补丁和更新以阻止威胁极为重要。

✓ 补丁是修复特定问题的一小段代码。

✓ 更新则可能包含要添加到软件包中的附加功能、以及针对特定问题的补丁。

- 操作系统和应用程序厂商会不断提供更新和安全补丁，以更正其已知的漏洞。此外，厂商通常还会发布补丁和更新的集合，称为服务包（Service Pack，SP）。许多操作系统都有自动更新功能，可以在主机上自动下载和安装操作系统及相关应用程序的更新。

# 3、防病毒软件

- 即使操作系统和应用程序应用了所有最新补丁和更新，仍然容易遭到攻击。任何连接到网络的设备都可能感染上病毒、蠕虫和特洛伊木马。这些攻击会损坏操作系统代码、影响计算机性能、更改应用程序和毁坏数据。

- 感染病毒、蠕虫或特洛伊木马后，可能出现的症状有：

  - ✓ 计算机行为开始变得不正常
  - ✓ 程序不响应鼠标和按键
  - ✓ 程序自行启动或关闭
  - ✓ Email程序开始外发大量Email
  - ✓ CPU使用率非常高
  - ✓ 有不认识的、或大量进程运行
  - ✓ 计算机速度显著下降或**崩溃（如蓝屏）**

- 防病毒软件可用作预防工具和反应工具。
- 它可预防感染，并能检测和删除病毒、蠕虫、特洛伊木马。连接到网络的所有计算机都应安装防病毒软件。市面上有多种防病毒程序。
- 几种免费杀毒软件（均持续更新）：

✓090928 微软免费杀毒软件MSE1.0正式版

✓091020 360免费杀毒软件1.0正式版

✓110318 瑞星个人杀毒软件2011宣布永久免费

✓浙大信息中心向全校师生提供免费网络安全服务：

趋势科技TREND MICRO → 360天擎校园版(企业版)防病毒系统（目前已停止更新）

- 防病毒软件可具有以下功能：
  - ✓电子邮件检查 — 扫描传入和传出的电子邮件，识别可疑的附件。
  - ✓驻留内容动态扫描 — 在打开访问可执行文件和文档时对它们进行检查。
    （包括对内存的实时动态检查）
  - ✓计划扫描 — 可根据计划按固定间隔运行病毒扫描以及检查特定驱动器或整个计算机。
  - ✓自动更新 — 检查和下载已知的最新病毒特征码和样式，并可设为定期检查更新

# 4、反垃圾邮件

参见4.03版教材动画8.3.4.1

- 反垃圾邮件软件可识别垃圾邮件并执行相应操作（例如将其放入垃圾邮件文件夹或删除），从而为主机提供保护。此类软件可在计算机本地加载，也可由电子邮件服务提供商在其电子邮件服务器上加载。而许多ISP也提供垃圾邮件过滤器。
- 反垃圾邮件软件无法识别所有垃圾邮件，因此打开电子邮件时仍须非常谨慎（哪怕是熟人的）。
- 有时有用的电子邮件也会被错误地当作垃圾邮件处理了，所以应定期到垃圾邮件文件夹（另外如QQ邮箱的广告邮件文件夹）中进行人工检查。

- 除了使用垃圾邮件拦截器等反垃圾邮件软件外，还应使用其它预防措施来防止垃圾邮件传播：
  - ✓ 及时应用现有的操作系统和应用程序更新。
  - ✓ 定期运行防病毒程序，并始终保持最新版本。
  - ✓ 不要转发可疑的电子邮件。
  - ✓ 不要打开电子邮件附件，尤其是来自陌生人的附件。
  - ✓ 在电子邮件客户端软件中设置电子邮件规则，删除绕过反垃圾邮件软件的垃圾邮件。
  - ✓ 标识垃圾邮件来源，并将其报告给网络管理员以便阻隔该来源。
  - ✓ 将事件报告给处理垃圾邮件滥用的政府机构。

# 5、反间谍软件

- 反间谍软件

✓ 间谍软件和广告软件也会导致类似病毒的症状。除收集未经授权的用户个人信息外，它们还会占用重要计算机资源并影响性能。

✓ 反间谍软件可检测和删除间谍软件，并防止它们将来再度安装。

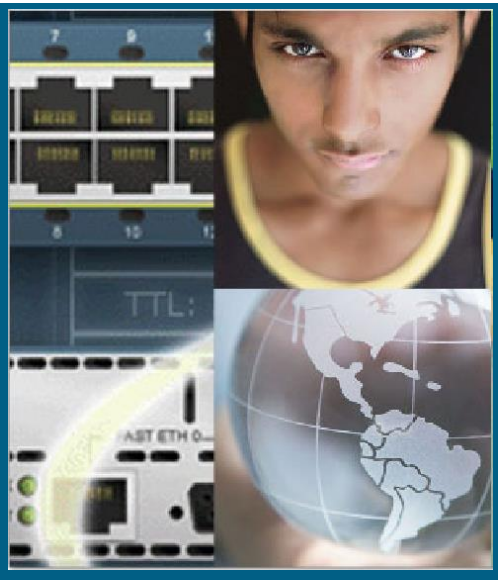
✓ 许多反间谍软件还包括Cookie及广告软件检测和删除功能。

✓ 目前某些防病毒软件包有反间谍软件功能。

## 弹出广告拦截器

- 可安装弹出广告拦截器软件来阻止弹出广告和背投广告。
- 许多Web浏览器默认包含弹出广告拦截器的功能。
- 但某些网站和程序会生成必要和有用的弹出窗口。因此很多弹出广告拦截器都有忽略功能（允许某些弹出窗口）。

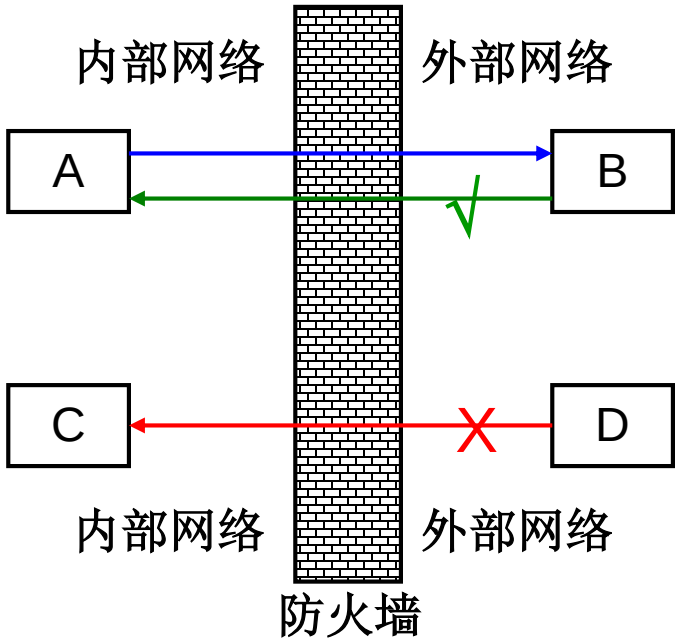
# 四、使用防火墙



# 1、什么是防火墙（7.02版16.3.5节）

- 防火墙是保护内部网络用户远离外部威胁最为有效的安全工具之一。
- 防火墙驻留在两个或多个网络之间，控制其间的通信量并帮助阻止未经授权的访问。
- 防火墙产品使用多种技术来区分应禁止和应允许的网络访问，包括：

- ✓ 数据包过滤：
  根据IP地址或MAC地址来阻止或允许访问。
- ✓ 应用程序/网站过滤：
  根据应用程序（即对应不同端口号的不同服务）来阻止或允许访问；网站过滤则通过指定要过滤的网站URL地址或关键字来实现。



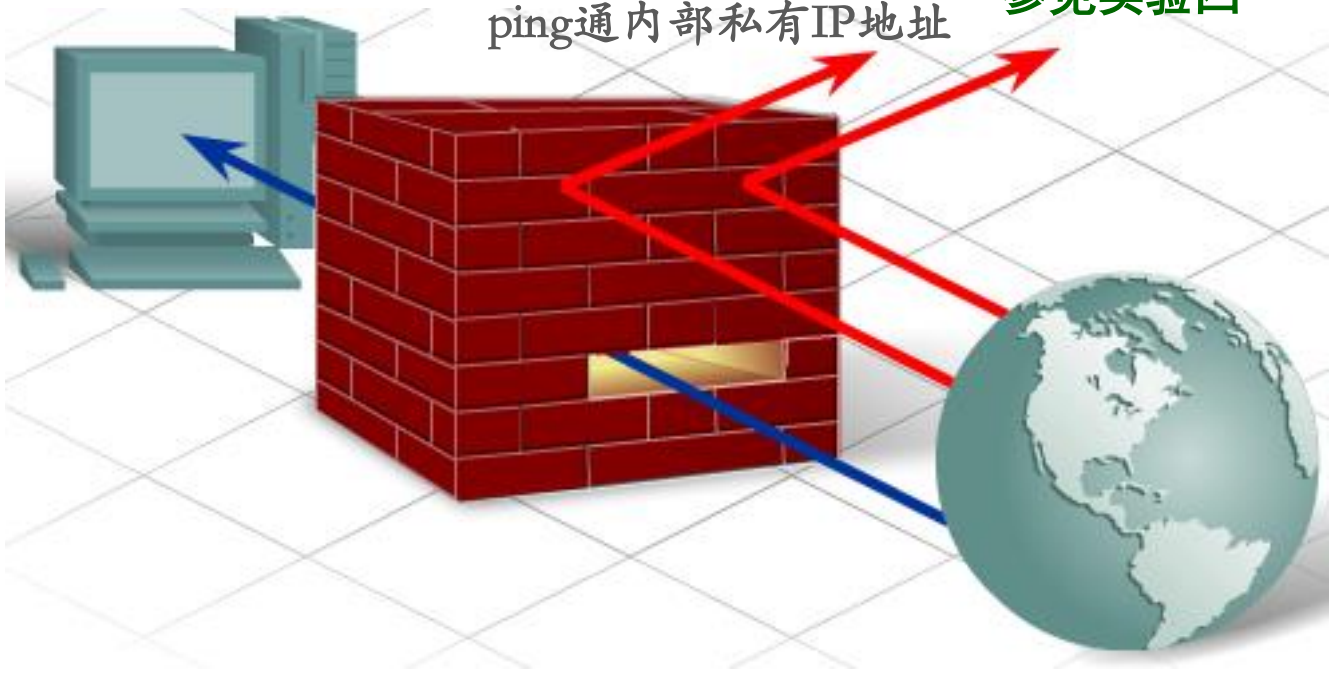

在线考试会考到

- 状态包侦测（SPI，也叫状态防火墙）：传入数据包必须是对内部主机所发出请求的合法响应才会被允许传入，否则未经请求的传入数据包会被阻隔。状态包侦测还可识别和过滤特定类型的攻击（如DoS攻击）。

- 此外，防火墙通常会执行网络地址转换(NAT)。NAT将一个或一组**内部私有地址**转换为一个**外部公有地址**，使用该公有地址可访问因特网，可实现对外部用户隐藏内部私有IP地址的目的。

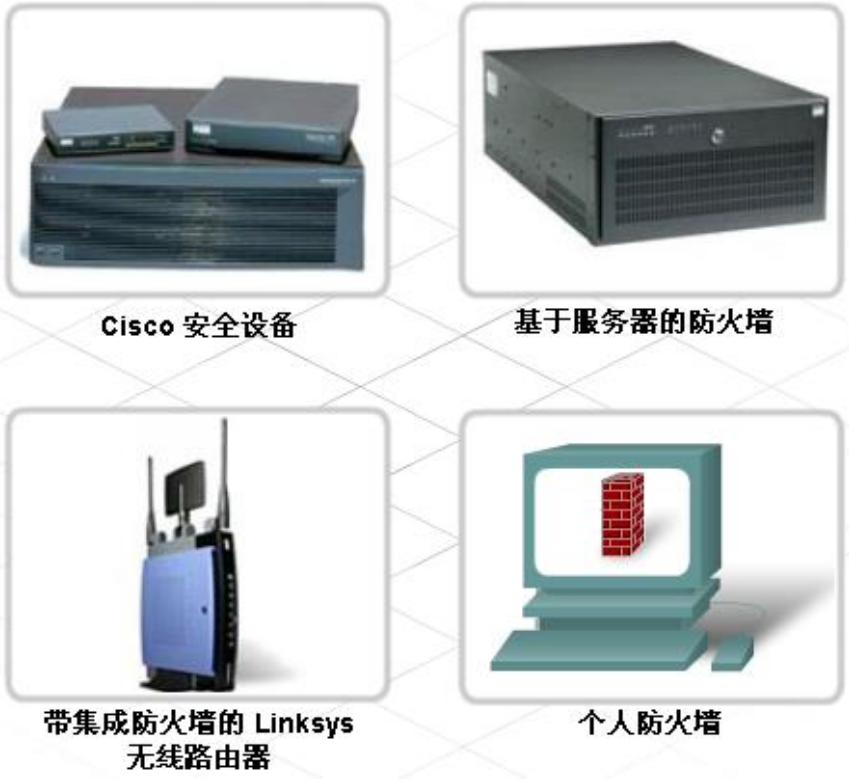
外部无法看见、无法直接ping通内部私有IP地址

参见实验四



（7.02版16.3.6节）

- 防火墙产品具有多种形式：
  - ✓ 基于设备的防火墙：内置于专用的硬件设备（称为安全设备）中，如Cisco PIX防火墙安全设备。
  - ✓ 基于服务器的防火墙：在已安装网络操作系统（NOS，如UNIX、Windows或Novell）的服务器上运行的企业网络防火墙应用程序。
  - ✓ 集成防火墙：通过对现有硬件设备（如路由器）添加防火墙功能来实现，如实验中的TP-LINK无线路由器里即有（参见实验四）。
  - ✓ 个人防火墙：驻留在主机计算机中的防火墙应用程序。可由操作系统提供，也可由外部厂商提供安装。




参见4.03版教材动画8.4.1.2

# 2、使用防火墙 （DMZ参见7.02版16.3.5节）

- 通过在内部网络和Internet之间设置防火墙作为边界设备，所有往来Internet的通信量都会被监视和控制。如此一来便在内部和外部网络间划分了一条清晰的防御界线。一般默认设置下，外部不能“看到”（直接访问或ping通）内部。
- 但有时可能会有一些外部客户需要访问内部资源，即需允许外访问内。为此可配置一个**非军事区(DMZ = DeMilitarized Zone)** **(参见实验四)** 。
- 术语**“非军事区”（也叫“非管制区”）**借用自军事用语，它代表两股势力间的一个指定区域，在该区域内不允许执行任何军事活动。

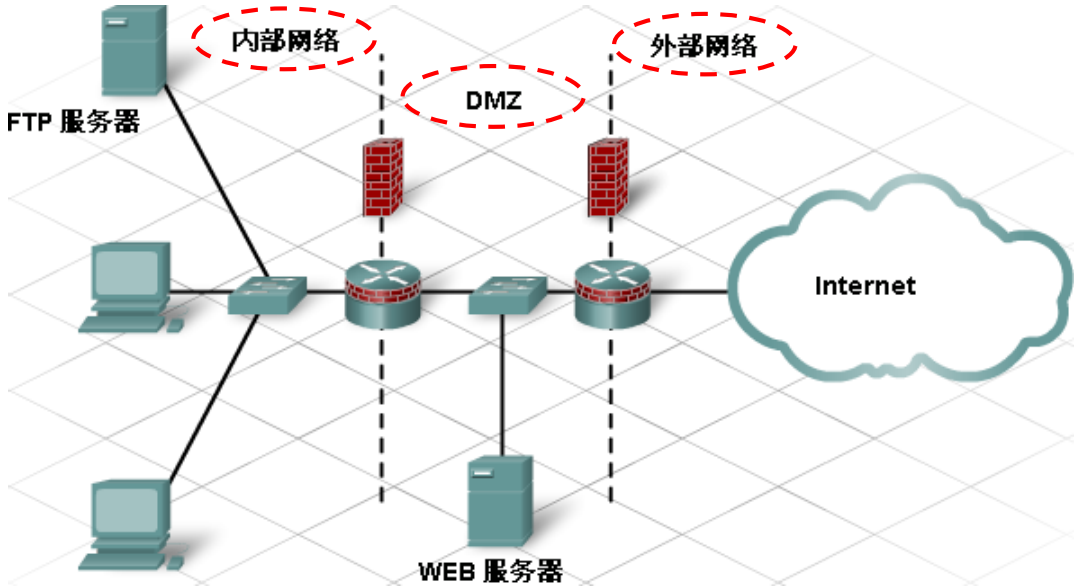
- 在计算机网络中，非军事区代表：
  内部和外部用户都可访问的网络区域。
  其安全性高于外部网络，低于内部网络。
- 它由一个或多个防火墙创建，这些防火墙起到分隔内部网络、非军事区和外部网络的作用。如用于公开访问的Web服务器通常就位于非军事区中。

参见4.03版教材动画8.4.2.1

- 双防火墙配置

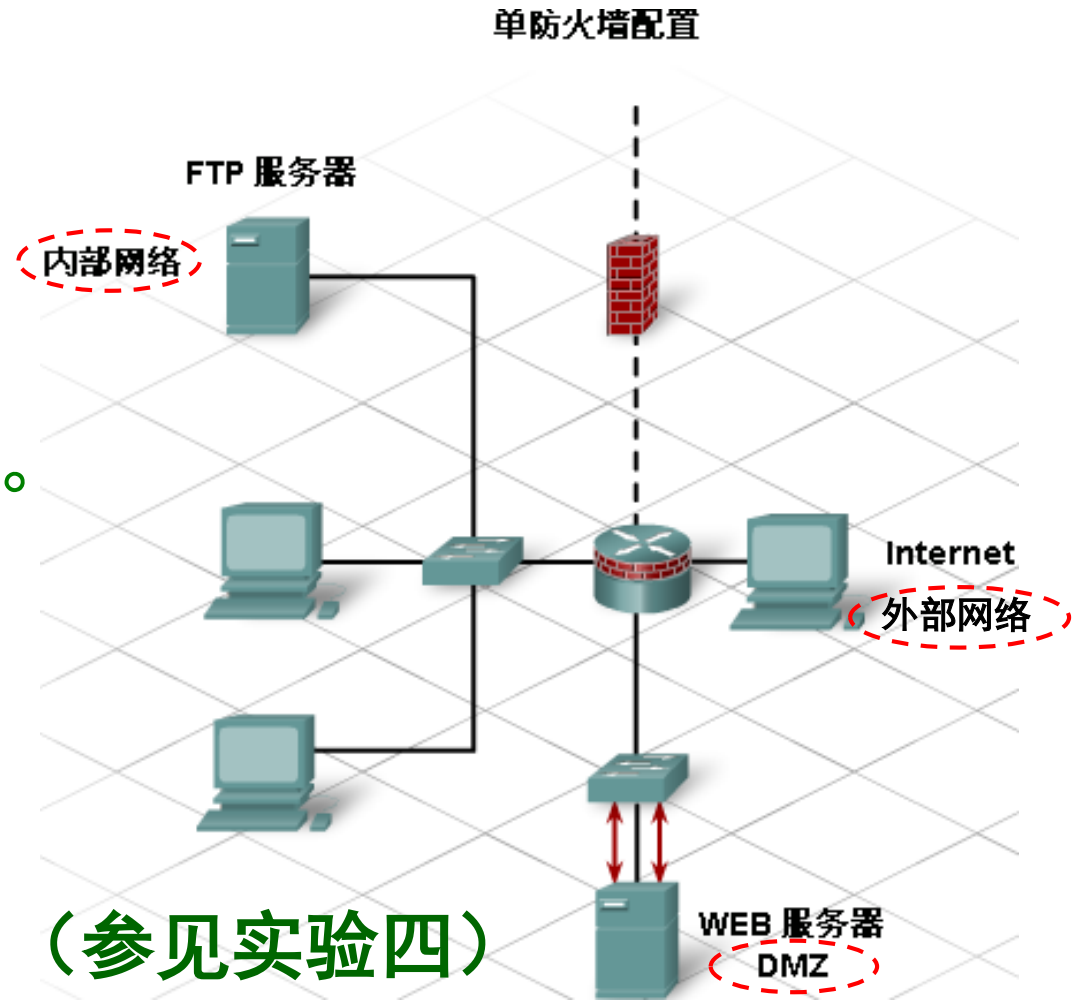
✓双防火墙配置中，防火墙分为内部防火墙和外部防火墙，其间则是非军事区。外部防火墙限制较少，允许Internet用户访问非军事区中的服务，而且允许任何内部用户请求的通信量通过。而内部防火墙则限制较多，用于保护内部网络免遭未经授权的访问。

双防火墙配置适合处理通信量较大的大型复杂网络。



- 单防火墙配置

✓单防火墙包含三个区域：外部网络、内部网络和非军事区。来自外部网络的所有通信量都被发送到防火墙。然后防火墙会监控通信量，决定哪些通信量应传送到非军事区，哪些应传送到内部网络，以及哪些应拒绝。




（参见实验四）

单防火墙配置适合规模较小、通信量较少的网络。

但是，单防火墙配置存在单一故障点，可能发生过载。

- 许多家庭网络设备（如实验中的TP-LINK集成无线路由器）都包含多功能防火墙软件：
  - 网络地址转换(NAT)
  - 状态包侦测(SPI)
  - IP地址、MAC地址、应用程序(服务端口号)及网站URL地址等过滤
  - 非军事区(DMZ) 及 端口转发(虚拟服务器)

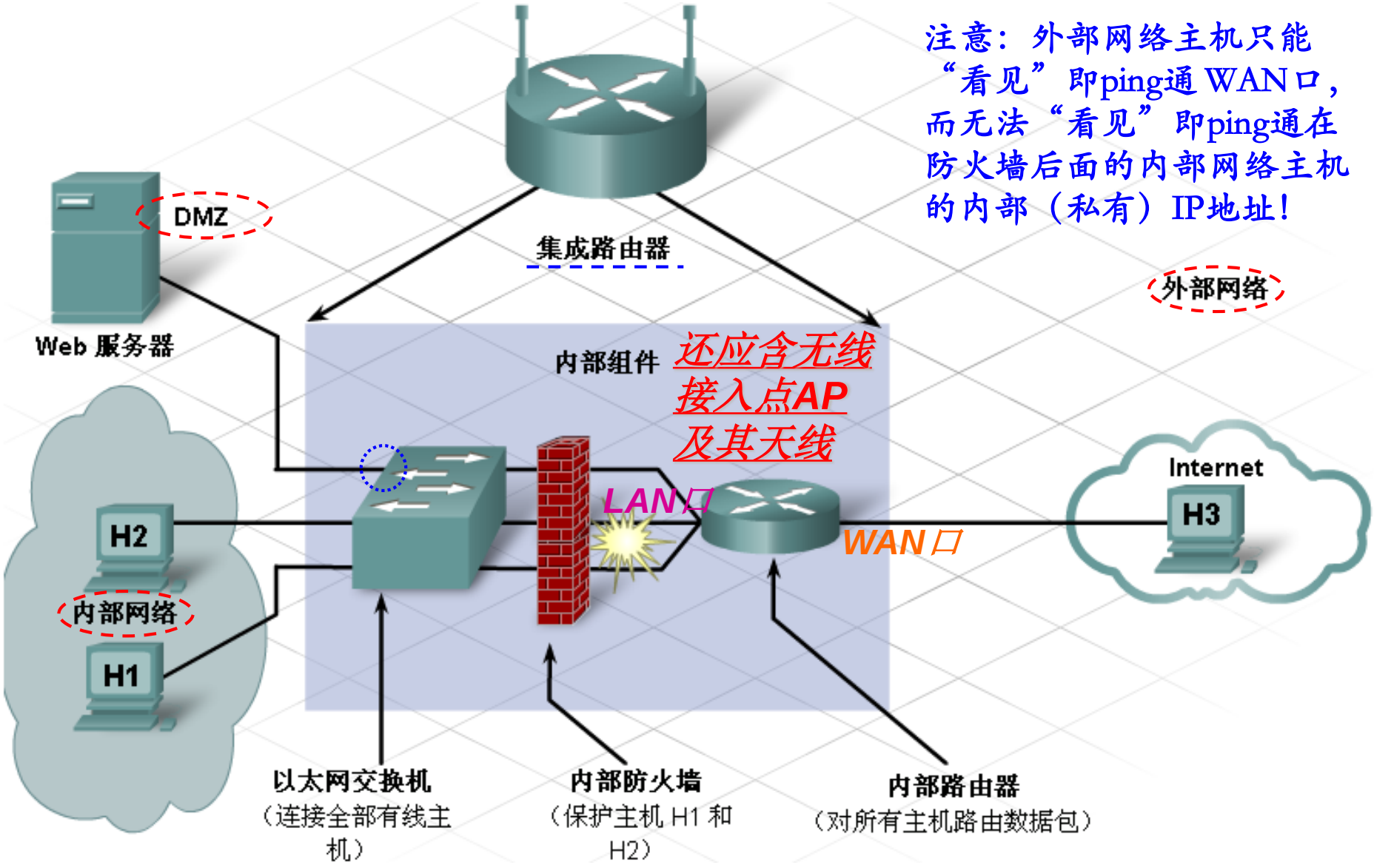
***只能间接访问（转发），无法直接访问（ping通）！***

- 在集成路由器中，可设置**非军事区DMZ**来允许外部网络主机访问内部网络中的服务器。为此，必须在集成路由器的**非军事区DMZ**配置中指定：欲允许外部访问的内部服务器的静态IP地址。
- 启用非军事区时，外部网络主机可访问内部网络中指定DMZ服务器的所有端口号上开设的服务，如80(HTTP)、21(FTP)和110(Email's POP3)等。
- 集成路由器会**隔离**以该指定DMZ服务器IP地址为目的地址的通信量（**注：其实外网访问时，目的地址形式上为WAN口地址**），然后这些通信量**会且仅会被转发到**该内部服务器所连接到的**内部交换机端口**上，进而再传到该内部服务器去**(如图所示)**；而所有其它内部主机仍受防火墙保护。

**参见实验四以更好理解！**

DMZ 端口转发

注意：外部网络主机只能“看见”即ping通WAN口，而无法“看见”即ping通在防火墙后面的内部网络主机的内部（私有）IP地址！



*只能间接访问（转发），无法直接访问（ping通）！*

- 另外，利用**端口转发**即**虚拟服务器**功能还可设置更具限制性的非军事区，服务器上的那些可访问端口均经特别指定。在此情况下，只有发送到这些端口的流量才获允许，其它流量则被排除。

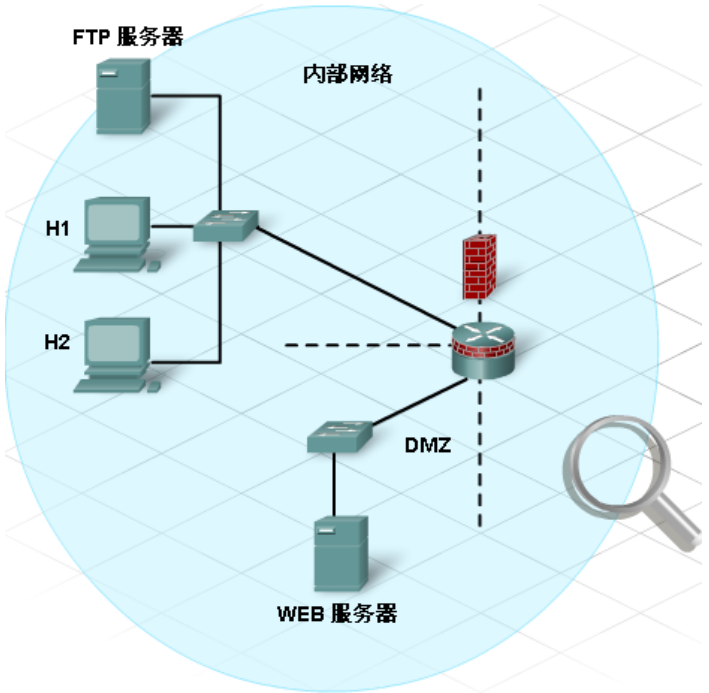
✓ 在集成路由器中，可设置**虚拟服务器**功能来允许外部网络主机访问内部网络中某一台服务器的某一个端口号上开设的服务。**参见实验四以更好理解！**

✓ 集成路由器会**隔离**以该内部服务器IP地址为目的地址、**以指定端口号为目的端口号**的通信量（**注：其实外网访问时，目的地址形式上也为 WAN口地址**），然后这些通信量**会且仅会被转发到**该内部服务器的**指定端口号**上去 **(如图所示)**；而该内部服务器的**其它端口号**及所有其它内部主机仍受保护。

➢ 宽带运营商可能屏蔽**80等常用服务端口**。在设置端口转发时，可修改外网用户访问的**外部端口**为运营商**非屏蔽端口如9000以上**，而**内部端口**仍可设为**80等所需服务端口**。

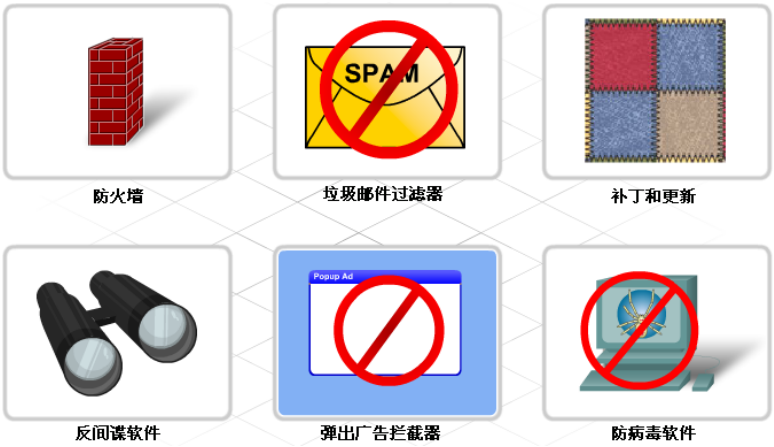
# 3、漏洞分析

- 有许多漏洞分析工具可用来测试主机和网络安全性。它们被称为安全扫描工具，帮助用户识别可能发生攻击的区域，并指导用户应采取哪些措施。尽管漏洞分析工具的具体功能随制造商的不同而有所不同，它们一些共同的功能包括：
  - ✓确定网络中可用主机的数目
  - ✓确定主机提供的服务
  - ✓确定主机上的操作系统和版本
  - ✓确定所使用的数据包过滤器和防火墙



# 4、最佳做法

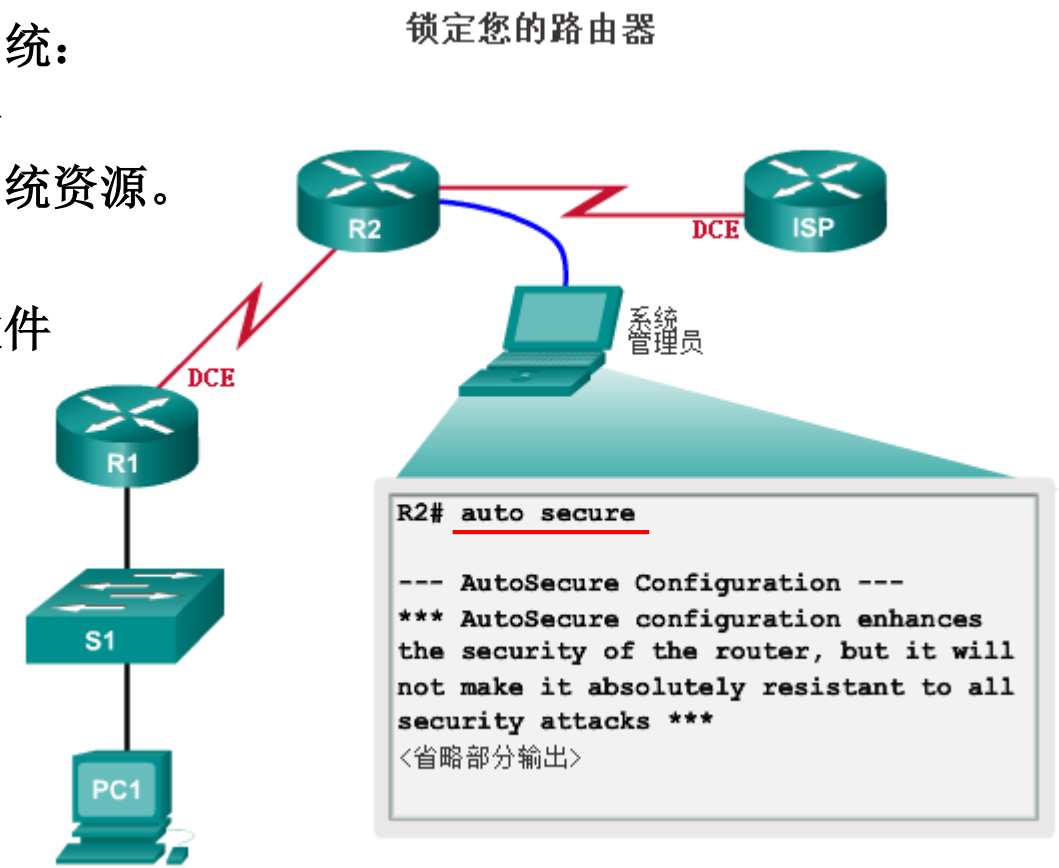
- 为缓解面对的风险，推荐采取以下措施：
  - ✓定义安全策略
  - ✓为服务器和网络设备提供物理防护
  - ✓设置登录和文件访问权限
  - ✓更新操作系统和应用程序
  - ✓更改许可的默认设置
  - ✓运行防病毒软件和反间谍软件
  - ✓更新防病毒软件文件
  - ✓激活浏览器工具—弹出广告拦截器、反网络钓鱼软件、插件监控器
  - ✓使用防火墙



# 7.02版 16.4节
# 设备安全

# 设备安全概述

- 当在设备上安装新的操作系统时，安全设置保留为默认值。
- 在大多数情况下，这种安全级别并不够。
- 对于思科路由器，Cisco AutoSecure 功能可用于协助保护系统，如图所示。
- 此外，以下各项适用于大多数系统：
  - 立即更换默认用户名和密码
  - 仅限获得授权的个人访问系统资源。
  - 关闭不必要的服务。
  - 在生产运作前，更新所有软件并安装所有安全补丁。



# 密码

- 使用强密码。强密码需遵循以下标准原则：（例如思科网院官网netacad的密码）
  - 至少 8 个字符，最好是 10 个或更多
  - 密码中混合使用大写和小写字母、数字、符号和空格
  - 无重复、无常见字典用字、无字母或数字序列、无用户名、亲戚、或宠物名称和其他容易识别的信息
  - 故意拼错的单词
  - 经常更改

| 弱密码 | 它为何弱 |
| --- | --- |
| secret | 简单词典密码 |
| smith | 母亲的婚前姓 |
| toyota | 汽车品牌 |
| bob1967 | 用户的姓名和生日 |
| Blueleaf23 | 简单的单词和数字 |

| 强密码 | 它为何强 |
| --- | --- |
| b67n42d39c | 组合使用字母数字字符 |
| 12^h u4@1p7 | 组合使用字母数字字符和特殊符号，并包括空格 |

# 基本安全实践

- 强密码只有在保持其机密性时才是有用的。

✓ **service password-encryption** 命令对配置中的密码进行加密。（7.02版模块2）

✓ **security passwords min-length** 命令确保所有配置的密码至少具有最短长度。

✓ **login block-for 120 attempts 3 within 60** 命令，
是在60秒内有3次失败的登录尝试时，屏蔽登录尝试120秒。
屏蔽连续的登录尝试有助于将对密码的暴力攻击降低到最低程度。

✓ **exec-timeout min. [sec.]** 命令设置线上空闲多长时间的用户将被自动断开。

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# exec-timeout 10
Router(config-line)# end
Router# show running-config
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

# 启用 SSH

- **Telnet** 并不安全。**强烈建议在设备上启用 SSH 以进行安全远程访问。**
- 对思科设备进行配置以支持 **SSH** 需要四个步骤：
  - 第 **1** 步：首先确保路由器具有唯一的（非默认）**hostname** 设备名称，然后在全局配置模式下使用 **ip domain-name** 命令配置网络的 **IP** 域名。
  - 第 **2** 步：使用 **crypto key generate rsa general-keys** 全局配置命令生成 **SSH** 密钥。
  - 第 **3** 步：使用 **username** 全局配置命令来创建本地数据库用户名条目。
  - 第 **4** 步：使用线路 **vty** 命令 **login local** 和 **transport input ssh** 启用传入 **SSH** 会话。（在线路子配置模式下）

# 启用 SSH（续）


**7.02版教材**
**16.4.4节例子**

第四次课
IOS命令示例中的
Router1即为如此
配置实现SSH访问

```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

```
第 1 步：配置 IP 域名。
第 2 步：生成单向密钥。
第 3 步：检验或创建本地数据库条目。
第 4 步：启用 VTY 传入 SSH 会话。
```

VTY线路配置中使用了 login 命令，包含关键字 local。这意味着，当用户从VTY线路（SSH/Telnet）进入用户模式时会要求用户先输入用户名和密码（来自于 username … secret … 命令）。

谢谢。

Cisco Networking Academy

Mind Wide Open