



北京大学网络攻防技术与实践课程

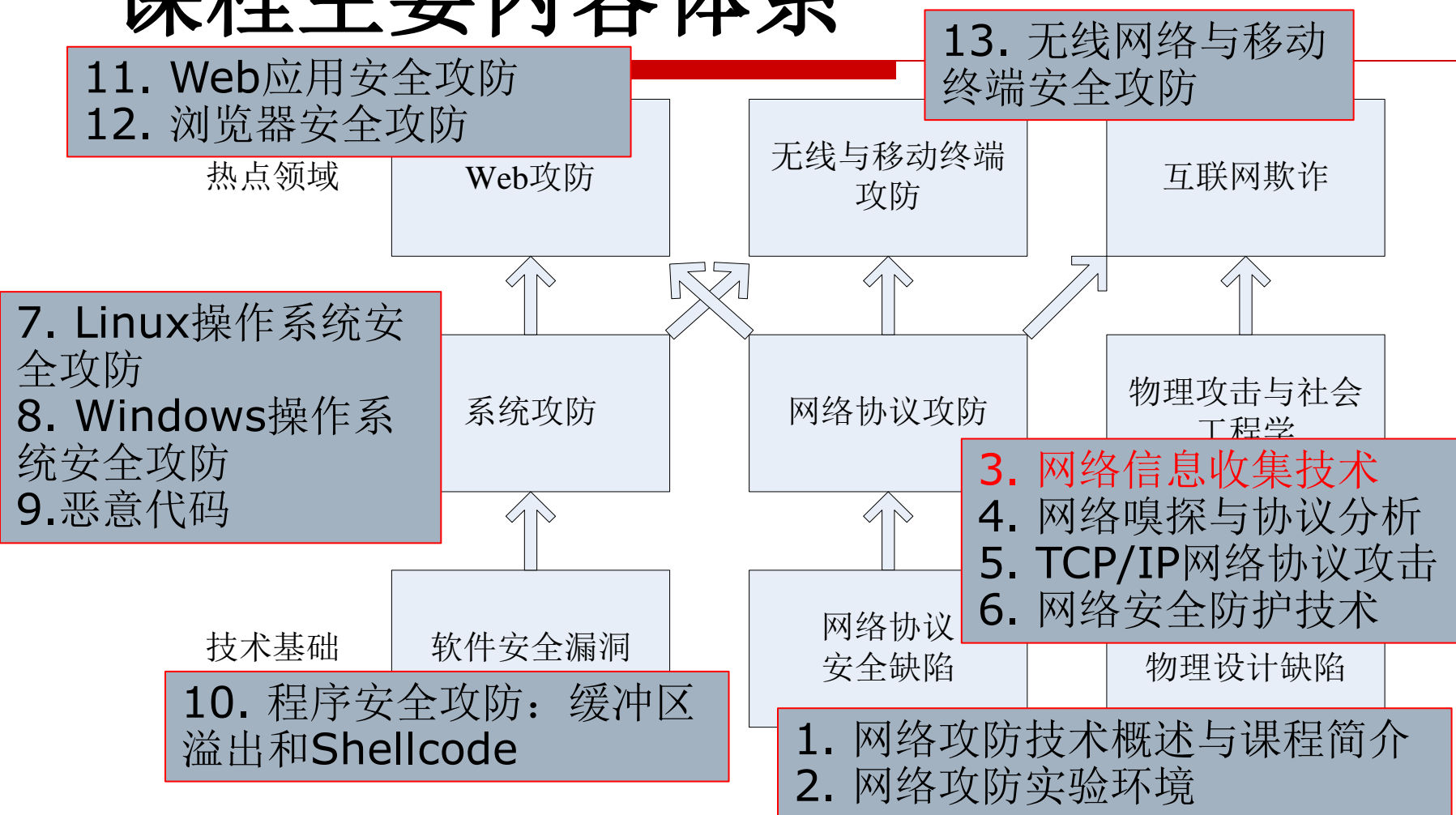
3. 网络信息收集技术(上)

诸葛建伟

zhugejianwei@icst.pku.edu.cn

北京大学计算机研究所信安中心

课程主要内容体系





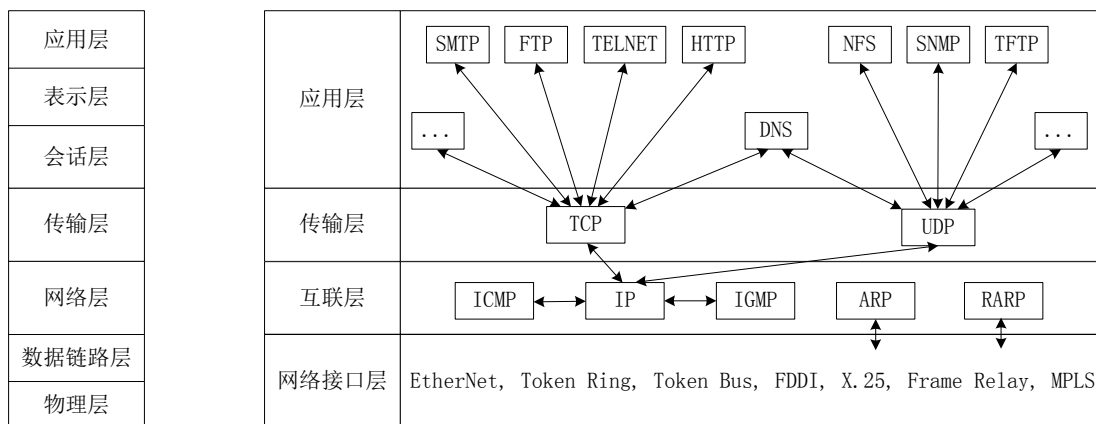
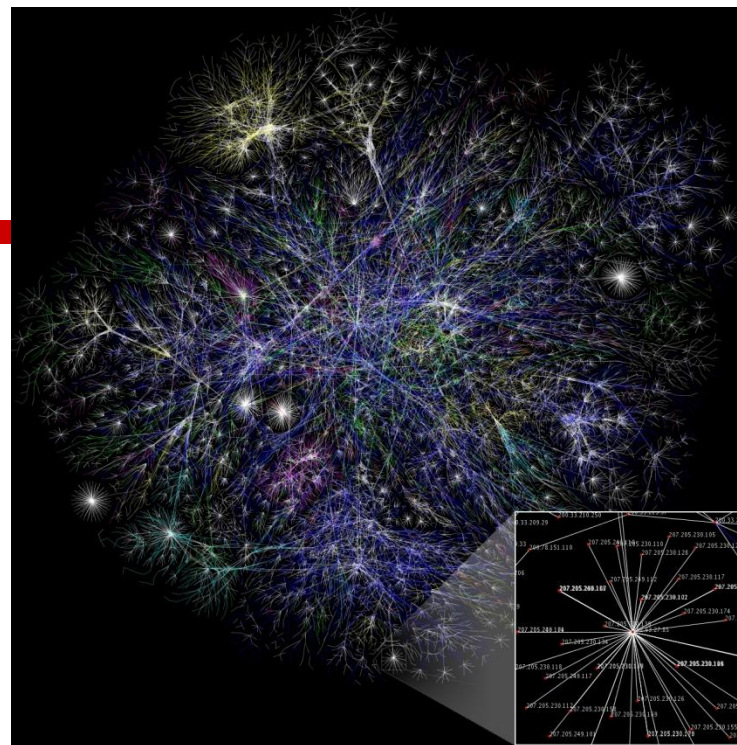
内容

1. 网络基础知识
2. 网络信息采集技术概述
3. 网络踩点技术
4. 课堂实践：DNS与IP查询
5. 网络扫描技术
6. 课堂实践：nmap扫描
7. 作业3—搜索自己的互联网足迹/网络扫描实验

网络基础知识

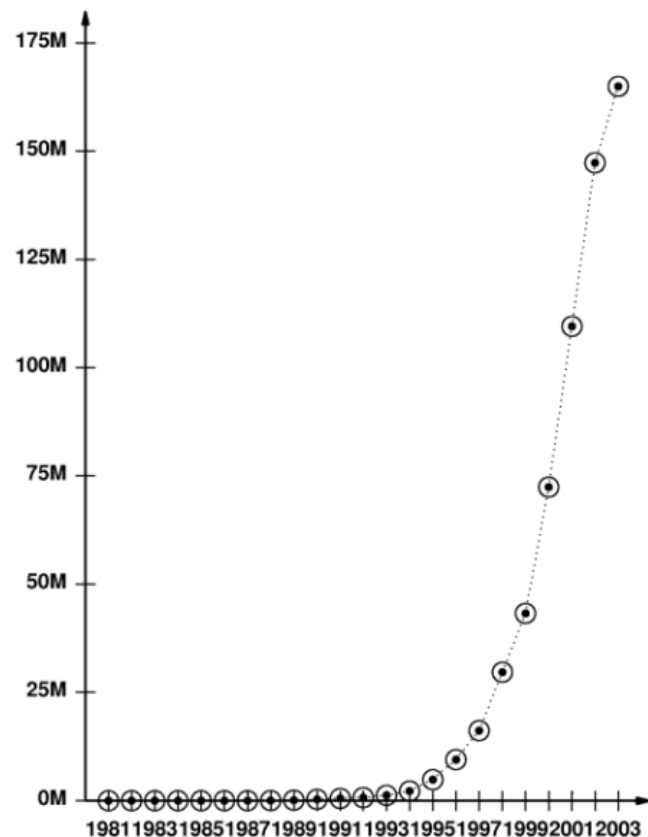
□ Internet

□ TCP/IP



Internet(因特网)起源

- **1969**年美国国防部**ARPANET**投入使用
- **1973**年**ARPANET**扩展成互联网，第一批接入的有英国和挪威。
- **1983**年**1月1日**，**ARPANET**将其网络内核协议由**NCP**改变为**TCP/IP**协议，独立出**MILNET**
- **1986**年**NSFNET**建立并连接**ARPANET**
- **1994**年商业运营，进入全球互联时代



1981到2003年间
每年接入**Internet**的计算机数目的增长速度

Internet的结构

Internet接入

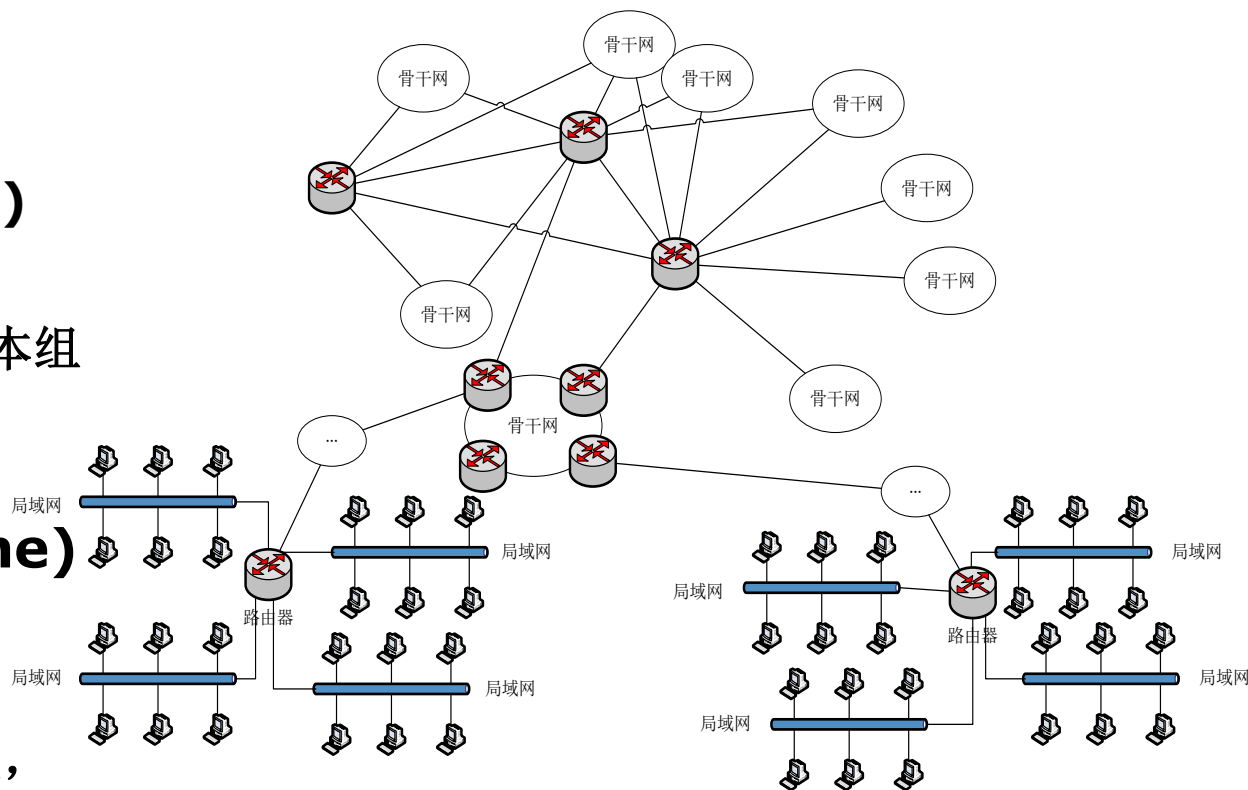
- 局域网
LAN(802.3)
- ADSL(PPPoE)

自治系统(AS)

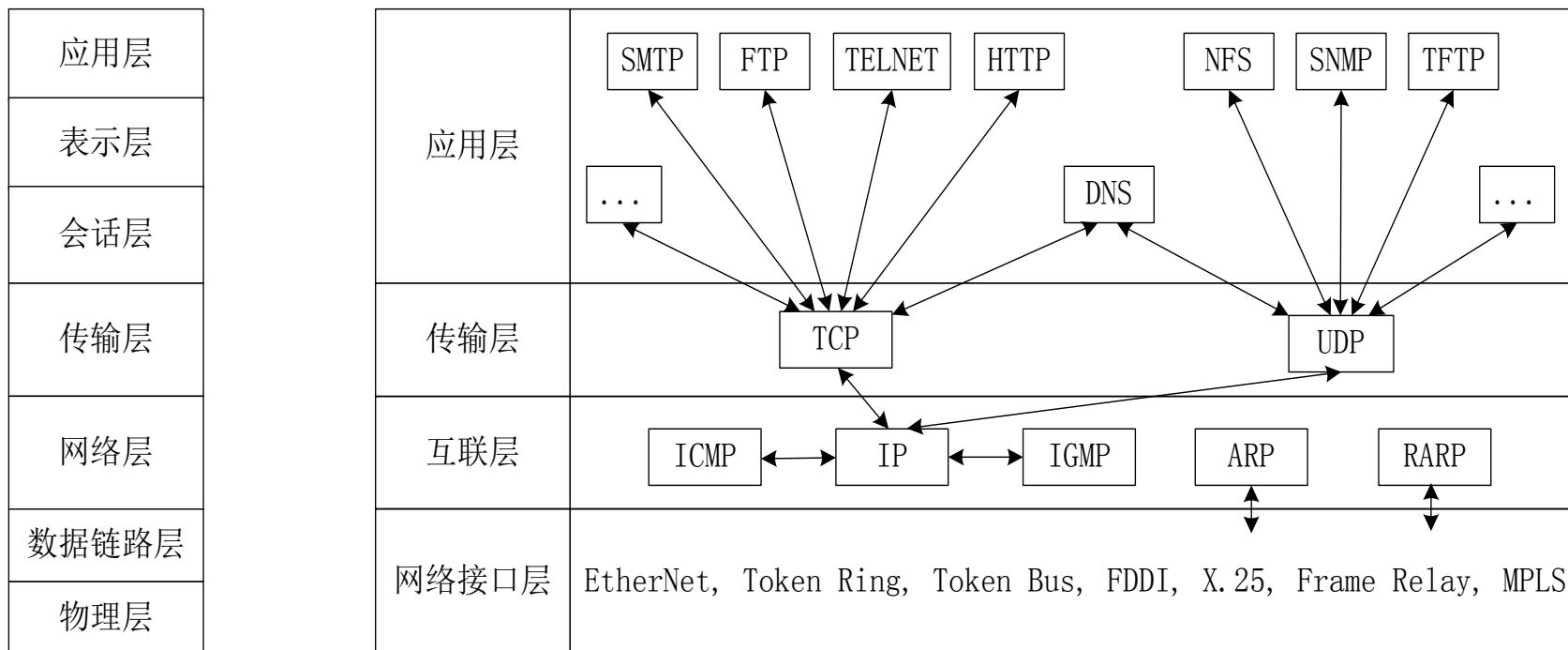
- Internet的基本组成单位
- ISP或大型组织

骨干网(Backbone)

- 大型网络中心
- 基础数据链路
- 地下、海底光缆, 冗余链路



TCP/IP协议栈



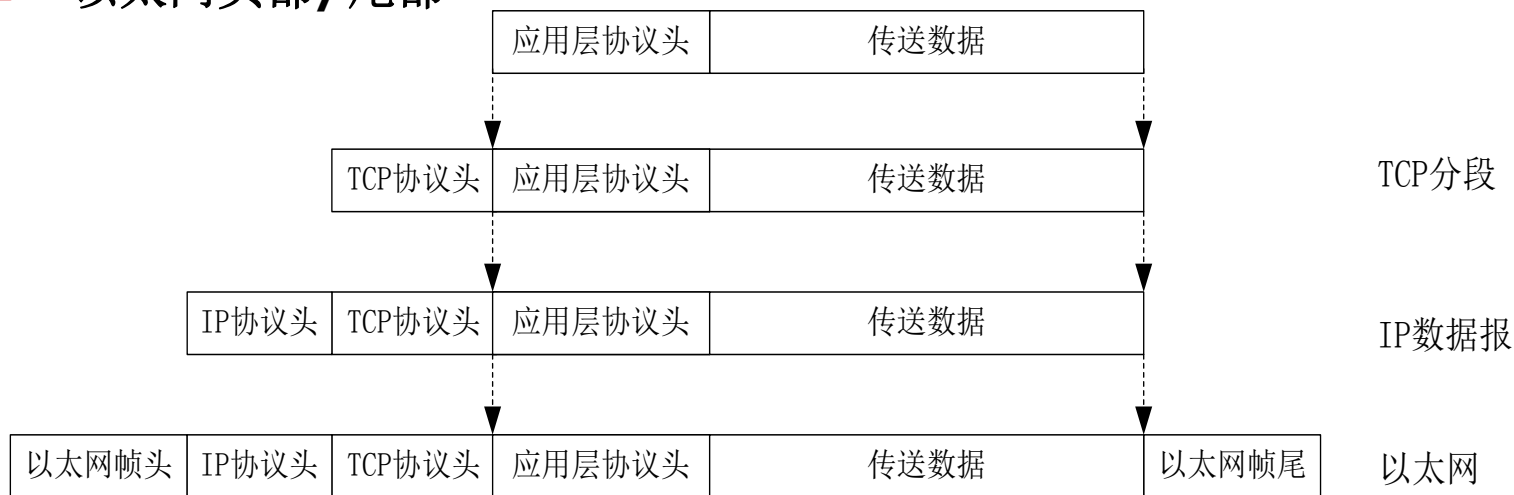
OSI模型各协议层

TCP/IP各协议层

TCP/IP协议栈典型封包过程

□ 数据包(帧)结构

- 传送用户数据—**payload**
- 应用层包头部
- **TCP/UDP**传输层头部
- **IP**网络层头部
- 以太网头部/尾部





IPv4数据包格式

0 3 4 7 8 15 16 18 19 31

版本号	报头长度	服务类型	总长度	
标识			标志	分段移位
生存期		协议	校验和	
源IP地址				
目的IP地址				
选项及填充				

IP网络互连的原理

□ 广播子网内部

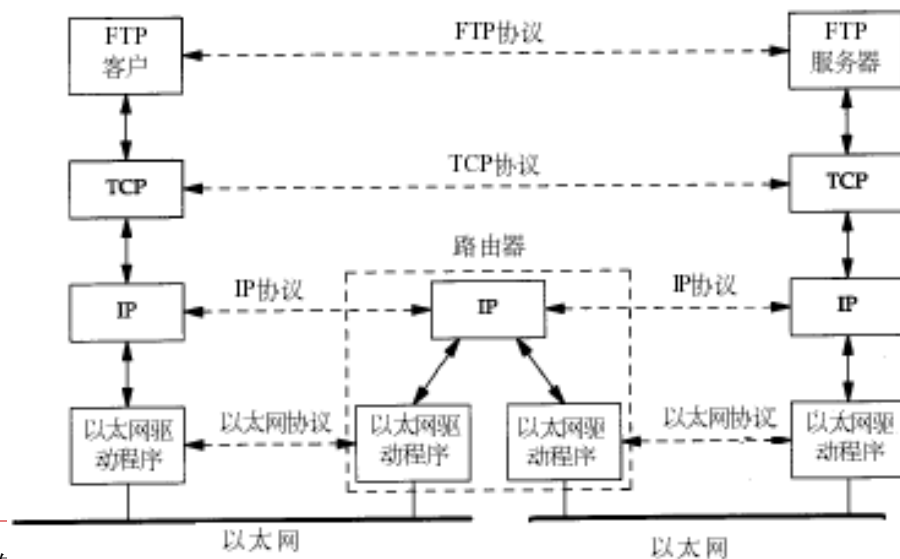
■ ARP地址解析

□ 从IP地址到MAC地址的解析

□ 子网间寻路—路由器

■ 路由协议BGP、

■ OSPF



TCP数据包格式

0	15															16	31														
源端口号																目的端口号															
序号																															
确认号																															
头部长度的长度		保留		URG		ACK		PSH		RST		SYN		PIN		窗口大小															
校验和																紧急指针															
选项及填充																															

- ❑ 序号(**SEQ**): 当前发送字节组的序号
- ❑ 确认号(**ACK**): 下一个要接收的字节组序号
- ❑ **TCP**协议实现可靠性传输的关键, 通过三次握手同步

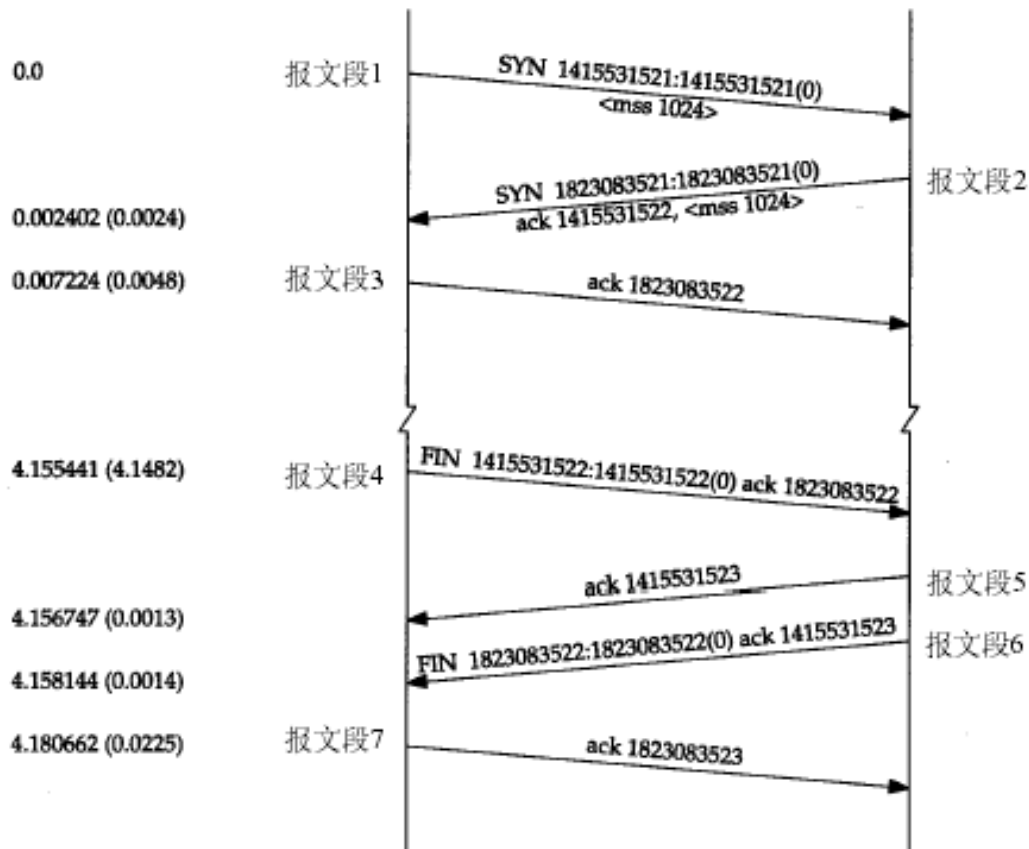
TCP协议连接交互过程

□ TCP-有状态的网络连接协议

- 可靠传输
- 拥塞控制
- 流模式

□ TCP三次握手

- C->S: SYN
- S->C: SYN|ACK
- C->S: ACK
- 协商SEQ/ACK





内容

1. 网络基础知识
2. 网络信息采集技术概述
3. 网络踩点技术
4. 课堂实践：DNS与IP查询
5. 网络扫描技术
6. 课堂实践：nmap扫描
7. 作业3—搜索自己的互联网足迹/网络扫描实验



网络信息收集的必要性

- “知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼，不知己，每战必殆。”
——《孙子·谋攻篇》。
- 攻防对抗(博弈)中：对敌方信息的掌握是关键
- 攻击者
 - 先手优势
 - 攻击目标信息收集
- 防御者
 - 后发制人？
 - 对攻击者实施信息收集，归因溯源



网络信息收集的内容

□ 网络攻击信息收集

- 入手点：目标的名称和域名
- 攻击准备阶段
 - 在网络中的“地理位置”
 - 与真实世界的联系（实施社工和物理攻击）
 - “网络地图”
 - 攻击所需的更详细信息
- 攻击实施阶段
 - 目标系统中存在的安全缺陷和漏洞
 - 目标系统的安全防护机制

□ 网络防御信息收集

- 追查入侵者的身份、网络位置、所攻击的目标、采用的攻击方法等
- 一般被归入取证与追踪技术范畴

网络信息收集的技术方法

踩点
Footprinting

扫描
Scanning

查点
Enumeration

信息收集

□ 网络踩点 (**footprinting**)

- Web搜索与挖掘
- DNS和IP查询
- 网络拓扑侦察

□ 网络扫描 (**scanning**)

- 主机扫描
- 端口扫描
- 系统类型探查
- 漏洞扫描

□ 网络查点 (**enumeration**)

- 旗标抓取
- 网络服务查点



内容

1. 网络基础知识
2. 网络信息采集技术概述
3. 网络踩点技术
4. 课堂实践：DNS与IP查询
5. 网络扫描技术
6. 课堂实践：nmap扫描
7. 作业3—搜索自己的互联网足迹/网络扫描实验



网络踩点一概要

□ 踩点(**footprinting**)

- 有计划、有步骤的信息情报收集
- 了解攻击目标的网络环境和信息安全状况
- 得到攻击目标剖析图

□ 踩点目的

- 通过对完整剖析图的细致分析
- 攻击者将会从中寻找出攻击目标可能存在的薄弱环节
- 为进一步的攻击行动提供指引



网络踩点针对的信息

□ 目标组织

- 具体使用的域名
- 网络地址范围
- 因特网上可直接访问的**IP**地址与网络服务
- 网络拓扑结构
- 电话号码段
- 电子邮件列表
- 信息安全状况

□ 目标个人

- 身份信息、联系方式、职业经历，甚至一些个人隐私信息



踩点能够获取的信息 – 案例

因特网

域名	pku.edu.cn
网络地址块	162.105.*.* /16, 222.29.0.0..222.29.159.255, 202.112.?.0/24
直接访问系统的具体IP	www.pku.edu.cn: 162.105.129.104 bbs.pku.edu.cn: 162.105.204.150 ... (https://its.pku.edu.cn/index.htm)
系统体系架构 百度百科: 北大未名BBS架设在64位x86服务器上, 软件则采用自行改造的Firebird BBS系统.
访问控制机制和相关访问控制表	构筑校园网安全保障体系. 张蓓, zhp@pku.edu.cn. 北京大学计算中心.
入侵检测系统	同上
各相关主机的细节信息
DNS主机名	pkuns.pku.edu.cn (162.105.129.27); sun1000e.pku.edu.cn (162.105.129.26); ns.pku.edu.cn (202.112.7.13)

内联网

各二级机构内部网络

...

远程访问

远程系统的类型	拨号入网, VPN
模拟/数字电话号码	拨号系统提供用户使用的电话号码是: 62751340、62751341、62751040, 拨号成功后, 可直接访问校内网络
身份验证机制	拨号入网采用教工工资号/密码进行身份验证 VPN采用北大校园网帐户/密码进行身份验证
VPN和相关协议配置	登陆地址: https://124.205.79.5/remote/login 采用协议配置: Fortinet SSL VPN



网络踩点技术手段

□ Web信息搜索与挖掘

■ “Google Hacking”

- 对目标组织和个人的大量公开或意外泄漏的**Web**信息进行挖掘

□ DNS与IP查询

- 公开的一些因特网基础信息服务
- 目标组织域名、**IP**以及地理位置之间的映射关系，以及注册的详细信息

□ 网络拓扑侦察

- 网络的网络拓扑结构和可能存在的网络访问路径

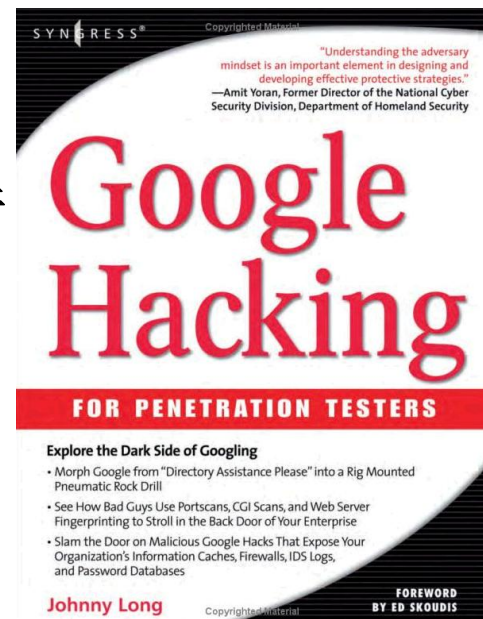
网络搜索

□ 公开渠道信息收集

- 目标**Web**网页、地理位置、相关组织
- 组织结构和人员、个人资料、电话、电子邮件
- 网络配置、安全防护机制的策略和技术细节

□ Google Hacking

- **Google Hacking:** 通过网络搜索引擎查找特定安全漏洞或私密信息的方法
- **allinurl:tsweb/default.htm:** 查找远程桌面**Web**连接
- **Johnny Long:** [Google Hacking Database](#)
- **Google Hacking软件:** Athena, Wikto, SiteDigger



Google Hacking 示例

Google Search: inurl:eStore/index.cgi?

rgod rates this entry 10 out of 10.
Submitted: 2006-08-13 00:00:00
Added by: rgod
Hits: 82
Score: 10

Google search: inurl: eStore/index.cgi?
路径遍历漏洞: URL../../../../etc/passwd

this is for eStore directory traversal, example exploit: [http://\[target\]/\[path\]/eStore/index.cgi?page=../../../../../../etc/passwd](http://[target]/[path]/eStore/index.cgi?page=../../../../../../etc/passwd)

Straw Beads - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 刷新 地址 http://birdstheword.com/cgi-bin/eStore/index.cgi?pid=183&cart_id=5346036.9410



Thursday, October 9, 2008 Total Quantity: 0 Subtotal: \$

Navigation

- Home
- About Us
- Contact Us
- Our Parrots
- Paypal
- Return Policy
- Shipping



We love these! They are hard plastic 'straw' beads onto leather laces or cords to make a fabulous addition you make for your birds.

birdstheword.com - toystore - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 刷新 地址 http://birdstheword.com/cgi-bin/eStore/index.cgi?page=../../../../../../etc/passwd



Thursday, October 9, 2008 Total Quantity: 0 Subtotal: \$ 0.00 View Cart

Navigation

- Home
- About Us
- Contact Us
- Our Parrots
- Paypal
- Return Policy
- Shipping

```
# $FreeBSD: src/etc/master.passwd,v 1.25.2.6 2002/06/30 17:57:17 des Exp $ #
root:*:0:0:Charlie &:/root:/bin/csh toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/sbin/nologin
operator:*:2:5:System &:/sbin/nologin bin:*:3:7:Binaries Commands and
Source:/sbin/nologin tty:*:4:65533:Tty Sandbox:/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/sbin/nologin games:*:7:13:Games pseudo-
user:/usr/games:/sbin/nologin news:*:8:8:News Subsystem:/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/sbin/nologin ftp:*:21:21:Anonymous FTP
```



如何用好Google-基本搜索技巧

□ 基本搜索与挖掘技巧

- 保持简单。简单明了的关键词更利于搜索。
- 使用最可能出现在要查找的网页上的字词。
- 尽量简明扼要地描述要查找的内容。
- 选择独特性的描述字词。
- 善于利用搜索词智能提示功能。

```
connectionString host=localhost dbname site:edu Search
About 26 results (0.08 seconds) Advanced search
Page Language="C#" Debug="true" trace="false" validateRequest ... ☆
Text="server=localhost;UID=sa;PWD=;database=master;Provider=SQLOLEDB"; ...
ConnectionString=Bin_SQLconnTextBox.Text; comm.Connection=conn; conn. ...
sxy edu.cn/downloads/conn.aspx - Cached
<script runat="server">
  public string Password="ce4a37e32bf88f054adc0ce2e6df24d0";
  public string SessionName="ASPXSpy";
  public string cookiePass="ASPXSpyCookiePass";
  public string Bin_Action="";
  public string Bin_Request="";
  protected OleDbConnection conn=new OleDbConnection();
```

源代码中泄漏数据库连接地址、口令与密码MD5值的例子

如何用好Google-高级搜索

高级搜索[搜索帮助](#)

搜索结果	包含全部字词	<input type="text"/>	10 项结果	<input type="button" value="Google 搜索"/>
	包含完整字句	<input type="text"/>		
	包含至少一个字词	<input type="text"/>		
	不包括字词	<input type="text"/>		
语言	搜索网页语言是	<input type="text" value="任何语言"/>		
地区	搜索网页位置于:	<input type="text" value="任何国家/地区"/>		
文件格式	<input type="button" value="仅"/> 显示使用以下文件格式的结果	<input type="text" value="任何格式"/>		
日期	返回在下列时间段内首次查看的网页	<input type="text" value="任何时间"/>		
字词位置	查询字词位于	<input type="text" value="网页内的任何地方"/>		
网站	<input type="button" value="仅"/> 搜索以下网站	<input type="text"/> 例如: .org, google.com 详细内容		
使用权限	搜索结果应	<input type="text" value="未经许可过滤"/>		

搜索特定网页

类似网页	搜索类似以下网页的网页	<input type="text"/> 例如: www.google.com/help.html	<input type="button" value="搜索"/>
链接	搜索与该网页存在链接的网页	<input type="text"/>	<input type="button" value="搜索"/>

Google信息搜索实例

-找出特定域名下尽可能多网站

❑ **allinurl:-php -html -htm -asp -aspx -ppt -pdf -swf -doc -xls site:pku.edu.cn**




allinurl:-php -html -htm -asp -aspx -ppt -pdf -swf

Search

About 78,500 results (0.10 seconds)

[Advanced search](#)

 Everything

 More

 Show search tools

Tip: [Search for English results only](#). You can specify your search language in [Preferences](#)

[欢迎访问北京大学主页](#) ☆ - [[Translate this page](#)]

北京大学作为国内前茅的文理医工综合性大学，在培养高素质创新型人才、取得突破性科研进展，以及为国民经济发展和社会进步提供智力支持等方面都发挥着极其重要的作用。

[www.pku.edu.cn/](#) - [Cached](#) - [Similar](#)

[北大美学：美学研究专业门户>> 网站首页](#) ☆ - [[Translate this page](#)]

所有学术专题, | 登陆 | 注册 | English | 所有文章, 美学大师, 新书推荐, 下载, 图片, 美学分类, 美学原理, 基本理论|前沿理论·马克思主义美学·外国美学 ...

[www.caae.pku.edu.cn/](#) - [Cached](#)

[北京大学高能物理研究中心](#) ☆ - [[Translate this page](#)]

北京大学高能物理研究中心, Center for High Energy Physics, Peking University.

[rchip.pku.edu.cn/](#) - [Cached](#) - [Similar](#)



Google信息搜索实例

-找出开放远程桌面Web连接的服务器

- 远程桌面Web连接-远程桌面的“Web版本”
- 可通过口令破解攻破设置了弱口令的服务器

The screenshot shows a Google search interface. The search bar contains the query 'allinurl:tsweb/default.htm site:cn'. Below the search bar, it indicates '2 results (0.15 seconds)' and a link to 'Advanced search'. On the left side, there are links for 'Everything', 'More', 'All results', 'Related searches', 'Page previews', and 'More search tools'. The search results list two items:

- [南昌\[REDACTED\]网络信息中心\[NIT\]---Remote Desktop Web Connection](#) ☆
- [Translate this page]
1600 then resWidth = 800 end if Response.Write resWidth %> HEIGHT=<% resHeight = Request.QueryString("rH") if resHeight < 200 or resHeight > 1200 then ...
[www.\[REDACTED\].edu.cn/tsweb/default.htm](#) - Cached
- [『荔乡\[REDACTED\]』远程桌面Web 连接](#) ☆ - [Translate this page]
1600 then resWidth = 800 end if Response.Write resWidth %> HEIGHT=<% resHeight = Request.QueryString("rH") if resHeight < 200 or resHeight > 1200 then ...
[www.\[REDACTED\].net.cn/tsweb/default.htm](#) - Cached

Google信息搜索实例

-尝试找出学生身份证号和信用卡信息

□ “filetype:xls 身份证号 site:edu.cn”

[\[xls\] 0829国家体育场残奥会志愿者保留名单.xls - 北京大学数学科学学院 ☆](#)
[- \[Translate this page \]](#)
 File Format: Microsoft Excel - [View as HTML](#)
 A, B, C, D, E, F, G, H, I, J, 1, 国家体育场残奥会赛时北京大学志愿者保留名单. 2, 场馆, 业务口, 分类, 预设岗位, 姓名, 校别, 院系, 备注, 上岗, 事由 ...
[www.math.pku.edu.cn:8000/.../0829国家体育场残奥会志愿者保留名单.xls - Similar](#)

配岗	院系	身份证号
国家体育场 sps	北大 中国语言文学系	2308 725
国家体育场 sps	北大 法学院	3601 03x
国家体育场 sps	北大 中国语言文学系	6323 11X
国家体育场 sps	北大 中国语言文学系	3601 024
国家体育场 sps	北大 中国语言文学系	5303 719
国家体育场 sps	北大 信息科学技术学院	4301 320
国家体育场 sps	北大 化学与分子工程学院	1101 522
国家体育场 sps	北大 历史学系	1101 518
国家体育场 sps	信息管理学系	1102 843
国家体育场 sps	地球空间科学学院	3625 034
国家体育场 sps	法学院	4105 154
国家体育场 sps	工学院	

□ “filetype:xls 信用卡 site:edu.cn”

A	B	C	D	E	F	G
学院	姓名	学号	信用卡1	信用卡2		
教师教育学院	阿·白合提亚尔	054 1 15	61 43			12
教师教育学院	白	074 4 15	49 43			23
教师教育学院	包	054 1 15	93 43			18
教师教育学院	包	064 1 15	83 43			76
教师教育学院	蔡	074 1 15	83 43			17
教师教育学院	陈	074 2 15	41 43			25
教师教育学院	陈	064 2 15	59 43			81

编程实现Web搜索

□ Google AJAX Search API

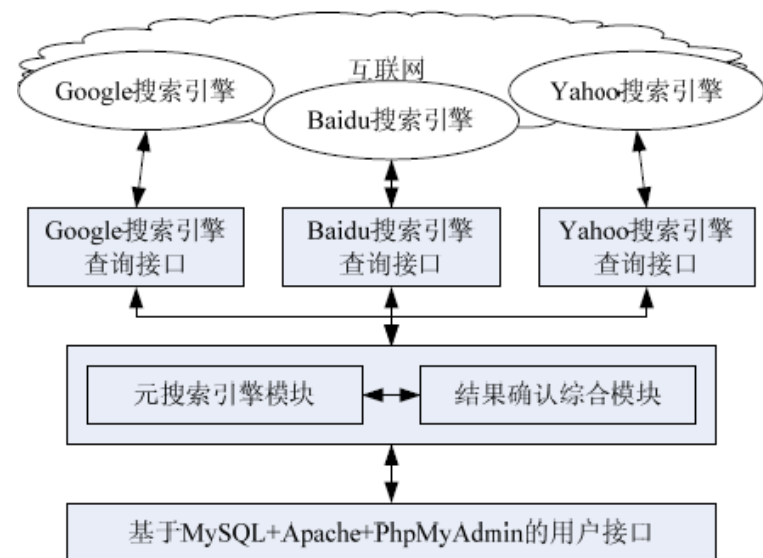
- Web网页和应用程序中集成Google搜索功能接口
- 只能返回64条结果

□ Xgoogle

- Python的Google搜索共享库
- 查询频率快会被Google认定程序自动搜索，CAPTCHA

□ 元搜索引擎

- 集成多个搜索引擎进行信息收集
- 基于元搜索引擎实现被篡改网站发现与攻击者调查剖析





Web信息搜索与挖掘防范措施

- 注意组织安全敏感信息以及个人隐私信息不要在因特网上随意发布
- 个人上网时尽量保持匿名
 - “网络实名制”？
 - 个人隐私权立法保护？还没有！
 - “跨省追捕”！
- 必须提供个人隐私信息时，应选择具有良好声誉并可信任的网站
- 定期对自身单位及个人在**Web**上的信息足迹进行搜索
 - 掌握**Google Hacking**信息搜索技术
 - 发现存在非预期泄漏的敏感信息后，应采取行动进行清除



公共信息服务

portal.pku.edu.cn/infoPortal/appmanager/myPortal/myDesktop?_nfpb=true&T3000671921159417872083_actionO



致力 构筑信息家园为北大人服务

快捷, 及时, 方便

Peking University

portal.pku.edu.cn

诸葛建伟, 欢迎登录信息门户!

首页

我的博客

我的校园卡

我的图书馆

联系我们

我的首页 个人信息 我的消息 新生入学 校务信息 公共信息 课程信息 人事业务 业务信息 财务信息 统计图表 仪器设备

人员查询

<< 返回查询界面

姓名	张慧琳	学号	10948893	准考证号	09487166
民族	回族	性别	女	出生日期	198[REDACTED]5
所在系	信息学院	专业	计算机应用技术	研究方向	互联网与信息安全
入学年月	200909	导师	邹维	学生类别	博士生
国籍	CHN	证件类型	身份证	证件号码	41[REDACTED]002x
政治面貌	中共党员	籍贯			

2011年6月28日

网络攻防技术与实践课程
Copyright (c) 2008-2009 诸葛建伟

31

DNS与IP查询 – DNS/IP基础设施

□ DNS/IP

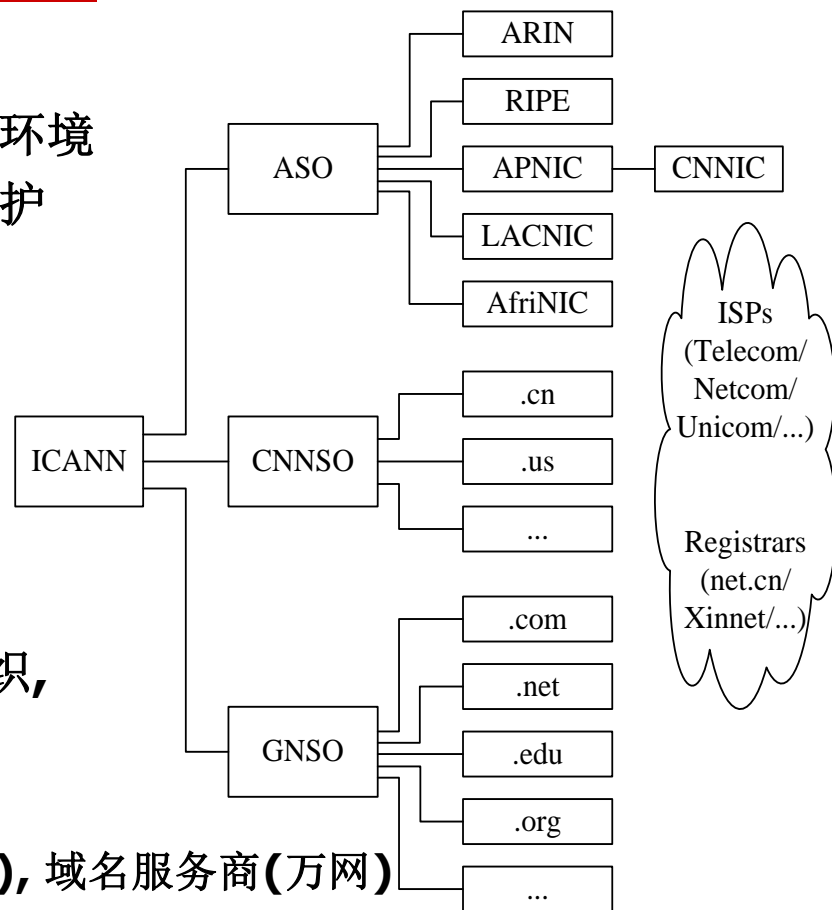
- 因特网赖以运转的两套基础设施环境
- 因特网上的公共数据库中进行维护
- 层次化结构管理

□ ICANN: 因特网技术协调机构

- **ASO**: 地址支持组织, 负责**IP**地址分配和管理
- **GNSO**: 基本名称支持组织, 负责通用顶级域名分配
- **CNNSO**: 国家代码域名支持组织, 负责国家顶级域名分配

□ 国内

- 公网: **CNNIC**, **ISPs**(电信, 网通...), 域名服务商(万网)
- 教育网: **CERNET**, 赛尔网络, ...





DNS注册信息Whois查询

□ 域名注册过程

- 注册人(**Registrant**) → 注册商(**Registrar**) → 官方注册局(**Registry**)
- **3R**注册信息: 分散在官方注册局或注册商各自维护数据库中
- 官方注册局一般会提供注册商和**Referral URL**信息
- 具体注册信息一般位于注册商数据库中

□ **WHOIS**查询

- 查询特定域名的**3R**详细注册信息
- 域名注册信息查询: **ICANN(IANA)** → 域名官方注册局 → 域名服务商
- **Whois Web**查询服务: 官方注册局、注册商
- 寻找域名注册信息数据库并查询返回结果的**Whois Web**查询服务: 万网、站长之家(whois.chinaz.com)
- 集成工具: **Whois**客户程序, **SamSpade**, **SuperScan**, ...



Whois查询示例-baidu.com

- ❑ **ICANN Whois**服务对**baidu.com**的查询结果
 - **Registrar:** REGISTER.COM, INC.
 - **Whois Server:** whois.register.com
 - **Referral URL:** <http://www.register.com>
- ❑ **Register.com Whois**服务对**baidu.com**的查询结果
 - **Registrant:**
Beijing Baidu Netcom Science and Technology Co.Ltd
 - **Administrative Contact:**
Beijing Baidu Netcom Science and Technology Co.Ltd.
...
Email: shaohui@baidu.com
 - **DNS Servers:**
ns.baidu.com, ns2.baidu.com, ns3.baidu.com



DNS服务：从DNS到IP的映射

□ DNS服务器和查询机制

■ 权威DNS服务器：提供原始DNS映射信息

- 主(primary)DNS服务器

- 辅助(secondary)DNS服务器

■ 递归缓存DNS服务器：ISP提供接入用户使用

- 分布式缓存与递归查询的机制

□ DNS查询工具

■ nslookup/dig



nslookup和dig

使用nslookup查询baidu.com	使用dig查询baidu.com
<pre>C:\Documents Settings\Administrator>nslookup *** Can't find server name for address 172.3*.**2.11: Non-existent domain *** Can't find server name for address 172.3*.**2.10: Non-existent domain *** Default servers are not available Default Server: UnKnown Address: 172.3*.**2.11 > www.baidu.com Non-authoritative answer: (非权威解答) Name: www.a.shifen.com Addresses: 119.75.213.50, 119.75.213.51 Aliases: www.baidu.com</pre>	<pre>administrator@administrator-desktop:~\$ dig @dns.baidu.com baidu.com ; <<>> DiG 9.7.0-P1 <<>> @dns.baidu.com baidu.com ; ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64527 ... ;; QUESTION SECTION: ;baidu.com. IN A ;; ANSWER SECTION(权威解答): baidu.com. 600 IN A 61.135.163.94 baidu.com. 600 IN A 220.181.6.81 baidu.com. 600 IN A 220.181.6.184 ;; AUTHORITY SECTION: baidu.com. 86411 IN NS ns3.baidu.com. ;; ADDITIONAL SECTION: dns.baidu.com. 300 IN A 202.108.22.220 ;; Query time: 4 msec ;; SERVER: 202.108.22.220#53(202.108.22.220) ;; WHEN: Sun Jul 25 11:17:59 2010 ;; MSG SIZE rcvd: 211</pre>

DNS区域传送

□ DNS区域传送

- nslookup: default server

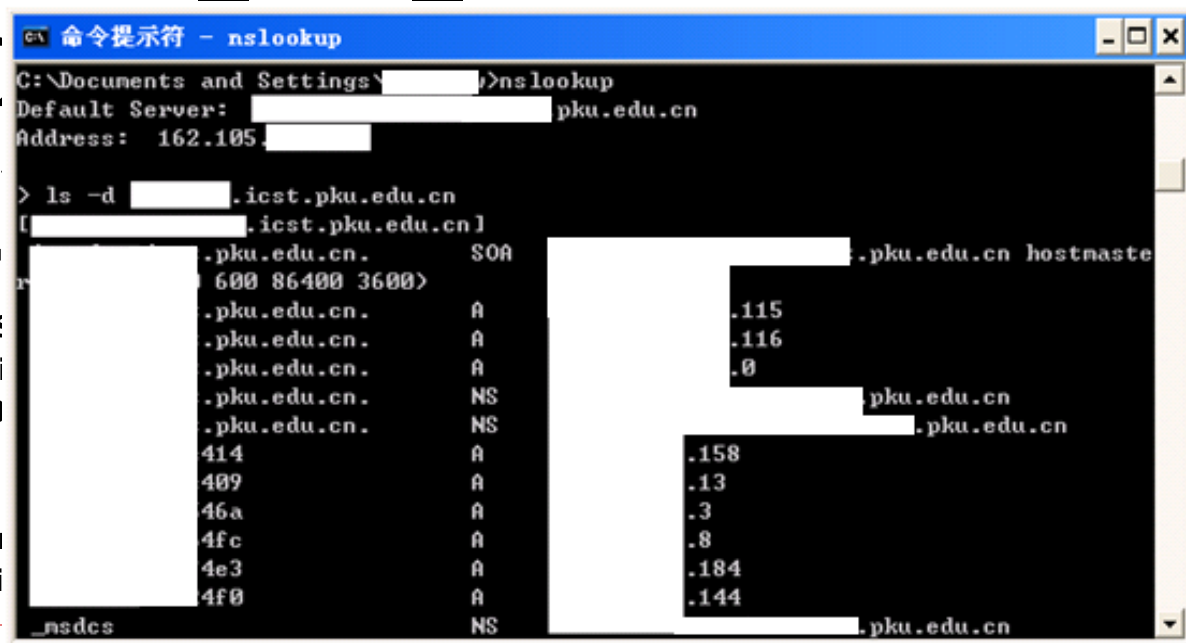
- ls -d DOMAIN_DNS_NAME

□ 阻断DNS区

- MMC控制
Transfer

- C:\Documents and S
- Default Server: gjjli
- Address: 202.106.0

- > ls -d bta.net.cn
- ls: connect: No error
- *** Can't list domain



```
命令提示符 - nslookup
C:\Documents and Settings\>nslookup
Default Server: pkpu.edu.cn
Address: 162.105.
> ls -d .icst.pkpu.edu.cn
[.icst.pkpu.edu.cn]
.pku.edu.cn. SOA .pkpu.edu.cn hostnaste
600 86400 3600>
.pku.edu.cn. A .115
.pku.edu.cn. A .116
.pku.edu.cn. A .0
.pku.edu.cn. NS .pkpu.edu.cn
.pku.edu.cn. NS .pkpu.edu.cn
414 A .158
409 A .13
46a A .3
4fc A .8
4e3 A .184
4f0 A .144
.nsdc NS .pkpu.edu.cn
```



IP Whois查询

□ IP分配过程

- **ICANN**的地址管理组织**ASO**总体负责
- 协调**RIR**和**NIR**进行具体分配与维护
- 每家**RIR**都知道每段**IP**地址范围属于哪家管辖
- 具体分配信息在**NIR/ISP**维护

□ IP Whois查询过程

- 任意**RIR**的**Whois**服务 (北美: **ARIN**, 亚太: **APNIC**)
- **162.105.1.1**查询示例
 - **ARIN**的**Whois Web**服务, 告知这段**IP**由**APNIC**管辖
 - **APNIC**的**Whois Web**服务, 给出该网段属于北大, 细节信息
 - 可能有时需要到**NIR(CNNIC)**或**ISP**查询更细致信息

□ 自动化程序和服务

- **Whois**客户程序

Whois客户程序示例

□ whois 162.105.163.116

```
[root@centos ~]# whois 162.105.163.116
[Querying whois.arin.net]
[Redirected to whois.apnic.net]
[Querying whois.apnic.net]
[whois.apnic.net]
% [whois.apnic.net node-1]
% Whois data copyright terms    http://w
```

```
inetnum:      162.105.0.0 - 162.105.255.
netname:      PUNET
descr:        imported inetnum object fo
country:      CN
admin-c:      XL151-AP
tech-c:       XL151-AP
status:       ALLOCATED PORTABLE
remarks:      -----
remarks:      imported from ARIN object:
remarks:
remarks:      inetnum:      162.105.0.0 - 162.105.255.255
remarks:      netname:      PUNET
remarks:      org-id:       PEKING
remarks:      status:      assignment
remarks:      rev-srv:      NS.PKU.EDU.CN
                        PKUNS.PKU.EDU.CN
                        SUN1000E.PKU.EDU.CN
remarks:      tech-c:      RS336-ARIN
remarks:      reg-date:    1992-09-30
remarks:      changed:     hostmaster@arin.net 20020920
remarks:      source:      ARIN
remarks:      -----
notify:       qj@pku.edu.cn
notify:       xnli@pku.edu.cn
mnt-by:       APNIC-HM
changed:      hostmaster@arin.net 20020920
changed:      hm-changed@apnic.net 20040926
changed:      hm-changed@apnic.net 20030616
changed:      hm-changed@apnic.net 20041214
source:      APNIC
```

Querying whois.arin.net
Redirected to whois.apnic.net
Querying whois.apnic.net



IP2Location—地理信息查询

□ IP2Location查询

- IP地址(因特网上的虚拟地址)→现实世界中的具体地理位置
- IP2Location数据库: WHOIS数据库, GeoIP, IP2Location, 纯真数据库 (QQ IP查询使用)

□ 地理信息查询

- Google Map, Sougou地图
- Google Earth



IP2Location示例

GeoIP



Support



My Account



FAQ



My Order

search

Home

GeoIP

minFraud

Contact

Company

GeoIP Demo

MaxMind GeoIP City/ISP/Organization Edition Results

Hostname	Country Code	Country Name	Region	Region Name	City	Postal Code	Latitude	Longitude	ISP	Organization	Metro Code	Area Code
222.29.112.10	CN	China	22	Beijing	Beijing		39.9289	116.3883	China Education and Research Network	Peking University New Campus		

纯真库

1.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
162.105.18.0 162.105.18.135 北京大学 数学系/心理系
162.105.18.136 162.105.18.136 北京大学 心理系认知实验室202
162.105.18.137 162.105.18.255 北京大学 数学系/心理系
162.105.19.0 162.105.19.255 北京大学 新地学楼(环境学院:自然/人文地理系)
162.105.20.0 162.105.20.255 北京大学 地质系/技术物理系/地球物理系
162.105.21.0 162.105.21.255 北京大学 物理系
162.105.22.0 162.105.22.255 北京大学 化学系
162.105.23.0 162.105.23.255 北京大学 地球物理系
162.105.24.0 162.105.24.255 北京大学 电教/文史楼
162.105.25.0 162.105.25.139 北京大学 力学系
162.105.25.140 162.105.25.140 北京大学 智能控制实验室(机器人、机器狗)
162.105.25.141 162.105.25.244 北京大学 力学系
162.105.25.245 162.105.25.245 北京大学 智能控制实验室
162.105.25.246 162.105.25.248 北京大学 力学系
162.105.25.249 162.105.25.249 北京大学 智能控制实验室(机器鱼)
162.105.25.250 162.105.25.255 北京大学 力学系
162.105.26.0 162.105.26.0 北京大学 电教楼/教育学院
162.105.26.1 162.105.26.255 北京大学 电子系
162.105.27.0 162.105.27.255 北京大学 化学与分子工程学院
162.105.28.0 162.105.28.255 北京大学 图书馆
162.105.29.0 162.105.29.44 北京大学 计算机系
162.105.29.45 162.105.29.45 北京大学 光华管理学院机房
162.105.29.46 162.105.30.255 北京大学 计算机系
162.105.31.0 162.105.31.255 北京大学 计算机中心机房
162.105.32.0 162.105.32.31 北京大学 45楼
162.105.32.32 162.105.32.32 北京大学 45楼2026
162.105.32.33 162.105.35.255 北京大学 45楼
162.105.36.0 162.105.38.255 北京大学 46楼
162.105.39.0 162.105.39.255 北京大学 46/47楼
162.105.40.0 162.105.43.255 北京大学 47楼
162.105.44.0 162.105.47.255 北京大学 48楼
162.105.48.0 162.105.48.255 北京大学 25楼
162.105.49.0 162.105.49.255 北京大学 30楼
162.105.50.0 162.105.51.255 北京大学 39楼
162.105.52.0 162.105.52.88 北京大学 33楼
162.105.52.89 162.105.52.89 北京大学 33楼一楼
162.105.52.90 162.105.52.255 北京大学 33楼
162.105.53.0 162.105.55.255 北京大学 33/34楼
162.105.56.0 162.105.56.255 北京大学 畅春新园4#
```

纯真IP数据库 (CZ88.NET)

IP=>地址

地址=>IP段

查询IP段

查询字段: 162.105.163.116

查询

IP : 162.105.163.116
地址: 北京大学 方正集团

本机IP

在线升级

解压

退出

请告知我们错误的IP地址、新IP地址,以便及时更新,谢谢! 金狐 CZ88.NET

2011年6月28日



Google Map & Google Earth

[网页](#) [图片](#) [地图](#) [资讯](#) [视频](#) [博客](#) [更多](#) ▼

[登录](#) [帮助](#)



方正大厦

搜索地图

[显示搜索选项](#)

查找互联网上的商户、地址和地点。 [了解详情。](#)

[公交 / 驾车](#)

[打印](#) [发送](#) [链接](#)

[文本视图](#) [地图视图](#)

Google Earth

File Edit View Tools Add Help

▼ Search

Fly To Find Businesses Directions

Fly to e.g., 94043

▼ Places Add Content

- My Places
- Sightseeing Select this folder and click on the 'Play' button below, to start the tour.
- Temporary Places

▼ Layers

- Primary Database
- Geographic Web
- Roads
- 3D Buildings
- Street View
- Borders and Labels
- Traffic
- Weather
- Gallery

方正大厦 (西门)

北京市海淀区
成府路298号

公交 / 驾车 - 在附近搜索
保存到“我的地图” - 发送

Image ©2008 GeoEye
© 2008 Europa Technologies

Google

39°59'22.23"N 116°18'36.37"E elev 53 m Jul 19, 2008 Eye alt 675 m

©2008 Google - 地图数据 ©2008 Mapabc.com - 使用条款



DNS与IP查询安全防范措施

- 公用数据库中提供信息的安全问题
 - 必须向注册机构提供尽可能准确的信息
- 采用一些安防措施不让攻击者轻易得手
 - 及时更新管理性事务联系人的信息
 - 尝试使用虚构的人名来作为管理性事务联系人
 - **“HoneyMan”**: 帮助发现和追查那些在电话或邮件中试图冒充虚构人名的“社会工程师”
 - 慎重考虑所列的电话号码和地址等信息
 - 注意域名注册机构允许更新注册信息的方式，并确保其中关键信息的安全
 - 攻击案例： **2008**年黑客进入了网络支付服务商**CheckFree**的邮箱，从而修改了域名记录

2010年1月12日百度“被黑”事件



李彦宏的i贴吧出现了一句其本人留言：
“史无前例，
史无前例呀！”



网络侦察

□ Traceroute – 路由跟踪

- 探测网络路由路径，可用于确定网络拓扑
- 主机发送**TTL**从**1**开始逐步增**1**的**IP**包，网络路径上路由器返回**ICMP TIME_EXCEEDED**
- **UNIX/Linux: traceroute**
- **Windows: tracert**
- 穿透防火墙: **traceroute -S -p53 TARGET_IP**
- 图形化界面工具: **VisualRoute, NeoTrace, Trout**

□ 网络侦察防范措施

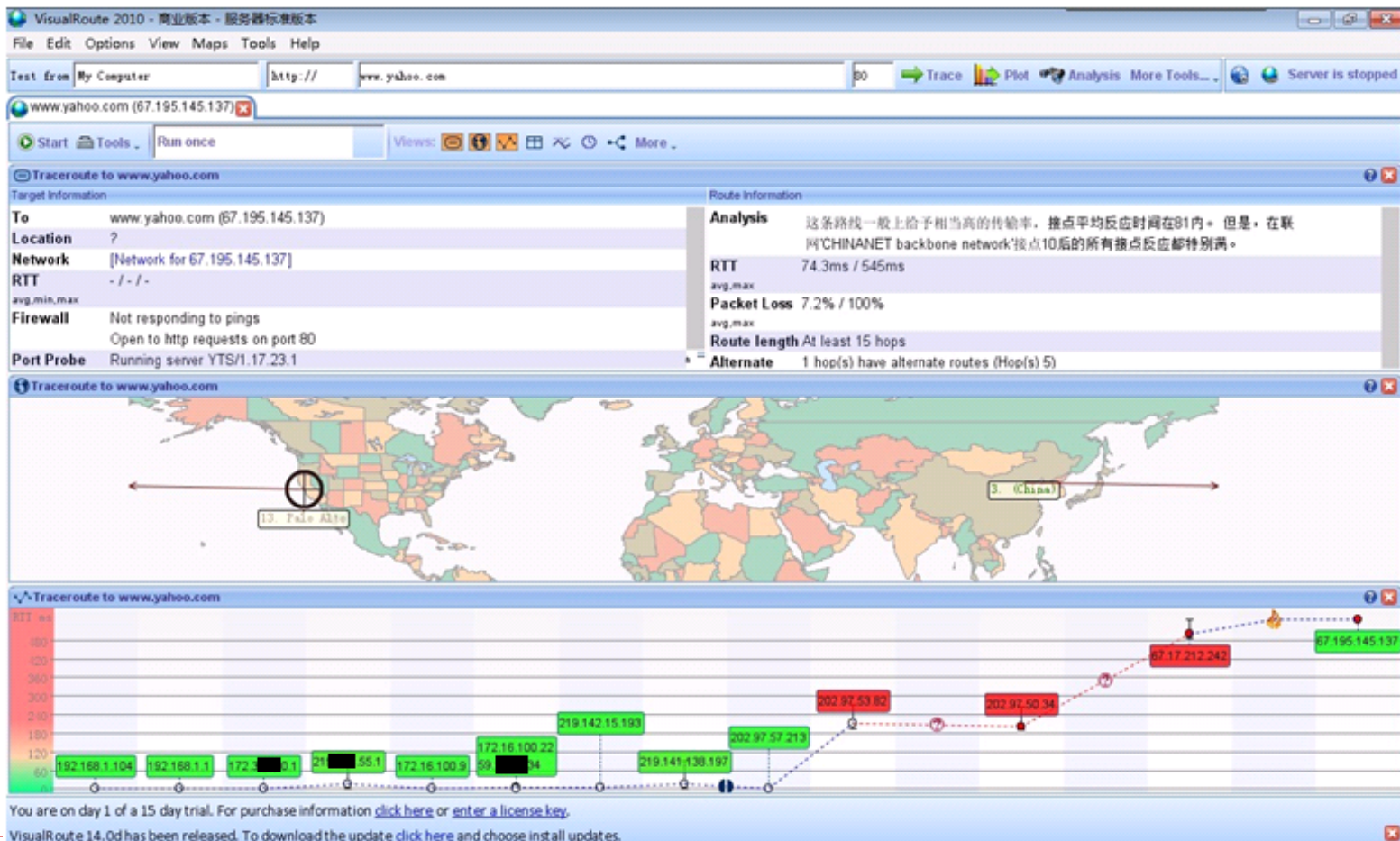
- 路由器配置: 只允许特定系统响应**ICMP/UDP**数据包
- 网络入侵检测系统/网络入侵防御系统: **Snort**
- 虚假响应信息: **RotoRouter**



Traceroute网络侦察示例

```
C:\Users\Administrator>tracert www.yahoo.com
Tracing route to yahoo.com[67.195.145.137]
over a maximum of 30 hops:
  1  2 ms  <1 ms  <1 ms  192.168.1.1
  2  1 ms   1 ms   1 ms  172.**.**0.1
  3  4 ms   2 ms   2 ms  219.***.*5.1
  4  7 ms   4 ms   3 ms  172.1*.***.*9
  5  4 ms   2 ms   2 ms  172.1*.***.*22
  6  3 ms   3 ms   4 ms  219.142.15.193
  7  5 ms   2 ms   2 ms  bj141-138-197.bjtelecom.net [219.141.138.197]
  8  2 ms   3 ms   2 ms  202.97.57.213
  9 45 ms  48 ms  46 ms  202.97.53.82
 10 *      *    185 ms  202.97.51.62
 11 191 ms 190 ms 190 ms 202.97.50.34
 12 189 ms 186 ms 185 ms 64.208.27.53
 13 425 ms 425 ms 423 ms YAHOO.TenGi3-4.1189.ar1.PAO2.gblx.net [67.17.212.242]
 14 424 ms *    425 ms UNKNOWN-216-115-107-73.yahoo.com [216.115.107.73]
 15 422 ms 423 ms *    ir2.fp.vip.sp1.yahoo.com [67.195.145.137]
 16 421 ms 422 ms *    ir2.fp.vip.sp1.yahoo.com [67.195.145.137]
 17 426 ms 423 ms 421 ms ir2.fp.vip.sp1.yahoo.com [67.195.145.137]
Trace complete.
```

图形化拓扑探测-VisualRoute





演示

- 利用网络踩点技术追踪“黑客”案例

- 网络踩点也非攻击者的专利技术
 - 防御和安全研究人员也可以利用
 - 对网络攻击者进行“人肉搜索”和“跨省追捕”



内容

1. 网络基础知识
2. 网络信息采集技术概述
3. 网络踩点技术
4. 课堂实践：DNS与IP查询
5. 网络扫描技术
6. 课堂实践：nmap扫描
7. 作业3—搜索自己的互联网足迹/网络扫描实验



Hands-on课堂实践(DNS与IP查询)

- 任务一：从**google.com**、**g.cn**、**baidu.com**、**sina.com.cn**中选择一个**DNS**域名进行查询，获取如下信息：
 - **DNS**注册人及联系方式
 - 该域名对应**IP**地址
 - **IP**地址注册人及联系方式
 - **IP**地址所在国家、城市和具体地理位置
- 任务二：尝试获取**BBS**、论坛、**QQ**、**MSN**中的某一好友**IP**地址，并查询获取该好友所在具体地理位置。
 - 提示：**QQ**、**MSN**在好友间进行较长时间的直接通讯时，将会建立起点到点的**TCP**或**UDP**连接，使用**netstat**命令或天网防火墙等工具，可获得好友的**IP**地址。



内容

1. 网络基础知识
2. 网络信息采集技术概述
3. 网络踩点技术
4. 课堂实践：DNS与IP查询
5. 网络扫描技术
6. 课堂实践：nmap扫描
7. 作业3—搜索自己的互联网足迹/网络扫描实验



网络扫描 V.S. 入室盗窃窥探

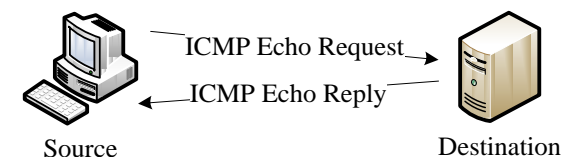
网络扫描类型	网络扫描目的	可对比的入室盗窃窥探步骤
主机扫描	找出网段内活跃主机	确定目标：找出大楼中有人住的房间
端口扫描	找出主机上所开放的网络服务	寻找门窗：找出可进入房间门窗位置
操作系统/ 网络服务辨识	识别主机安装的操作系统类型与开放网络服务类型，以选择不同渗透攻击代码及配置	识别房间、门窗等的材质类型，针对不同材质结构选择不同破解工具
漏洞扫描	找出主机/网络服务上所存在的安全漏洞，作为破解通道	缝隙/漏洞搜索：进一步发现门窗中可撬开的缝隙、锁眼

主机扫描(ping扫描)

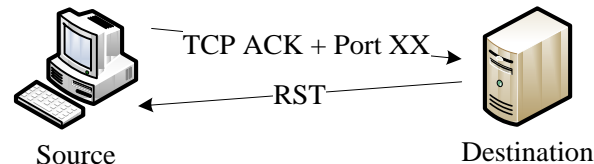
□ 主机扫描目的：检查目标主机是否活跃(**active**)。

□ 主机扫描方式

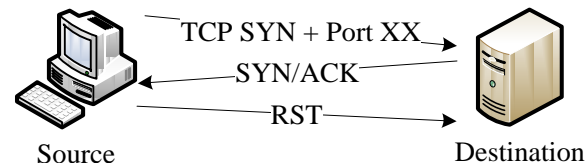
■ 传统**ICMP Ping**扫描



■ **ACK Ping**扫描

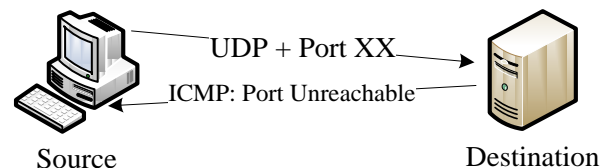


■ **SYN Ping**扫描



■ **UDP Ping**扫描：到关闭端口

□ 主机扫描程序



■ **Ping**

■ **Nmap: -sP**选项, 缺省执行,集合了**ICMP/SYN/ ACK/ UDP Ping**功能



Ping扫描

□ Ping扫描

- 同时扫描大量的IP地址段，以发现某个IP地址是否绑定活跃主机的扫描

□ Ping扫描工具软件

- **UNIX: Nmap, fping, hping2**
- **Win32: Superscan**

```
root@administrator-desktop:~# nmap -sP 172.**.*.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2010-2-22 23:27 CST
Host localhost (172.**.*.1) is up(0.00075s latency) .
MAC Address: 00:90:**:**:**:DE (Lanner Electronics)
Host localhost (172.**.*.2) is up(0.00047s latency) .
MAC Address: 00:90:**:**:**:B3 (Lanner Electronics)
Host localhost (172.**.*.3) is up(0.00037s latency) .
MAC Address: 00:22:**:**:**:6A (Dell)
Host localhost (172.**.*.4) is up(0.00035s latency) .
MAC Address: 00:14:**:**:**:58 (IBM)
...
Host localhost (172.**.*.210) is up (0.00052s latency) .
MAC Address: 00:50:56:94: 08:96 (VMWare)
Nmap done: 256 IP addresses (14 hosts up) scanned in 2.23 seconds
```



主机扫描防范措施

- 单一主机**Ping**扫描很常见，危害性也不大，更关注**Ping**扫射
- 监测：网络入侵检测系统**Snort**；主机扫描监测工具**Scanlogd**
- 防御：仔细考虑对**ICMP**通信的过滤策略
 - 利用**Ping**构建后门：**loki (Phrack v51#06)**, **pingd**



端口扫描技术

□ 端口

- **TCP/UDP (1-64K)**, 运行网络应用服务
- 由**IANA/ICANN**负责分配

□ 什么是端口扫描

- 连接目标主机的**TCP**和**UDP**端口, 确定哪些服务正在运行即处于监听状态的过程。

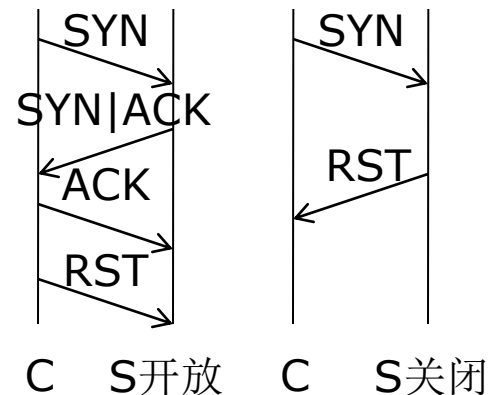
□ 端口扫描目的

- 防御者—更加了解所管理的网络状况, 找出没有必要开放的端口并关闭, 这是保证业务网络安全的第一步。
- 攻击者—找出可供进一步攻击的网络服务, 同时结合操作系统探测技术也可以确定目标主机所安装的操作系统版本。开放网络服务和操作系统版本信息为攻击者提供了破解攻击的目标, 使其更容易找出进入目标主机的漏洞路径。

TCP连接扫描, SYN扫描

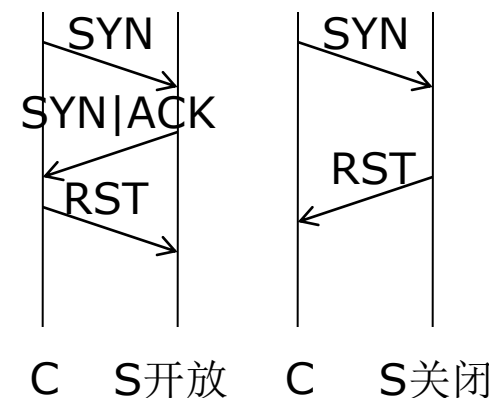
□ TCP连接扫描

- 调用**connect() socket**函数连接目标端口
- 开放端口：完成完整的**TCP三次握手(SYN, SYN|ACK, ACK)**, **timeout/RST**
- 关闭端口：**SYN, RST**
- 优势&弱势：无需特权用户权限可发起，目标主机记录大量连接和错误信息，容易检测



□ SYN扫描

- 半开扫描(**half-open scanning**)
- 开放端口：攻击者**SYN**, 目标主机**SYN|ACK**, 攻击者立即反馈**RST**包关闭连接
- 关闭端口：攻击者**SYN**, 目标主机**RST**
- 优势&弱势：目标主机不会记录未建立连接，较为隐蔽，需根用户权限构建定制**SYN**包





隐蔽端口扫描

□ 隐蔽端口扫描方式

- **TCP**连接扫描和**SYN**扫描并不隐蔽：防火墙会监控发往受限端口的**SYN**包
- 隐蔽端口扫描通过构造特殊的**TCP**标志位，以躲避检测，同时达成端口扫描目的。
- **FIN**扫描(只带**FIN**位), **Null**扫描(全为**0**), **XMAS**扫描(**FIN/URG/PUSH**)
- **FTP**弹射扫描：利用**FTP**代理选项达到隐蔽源地址

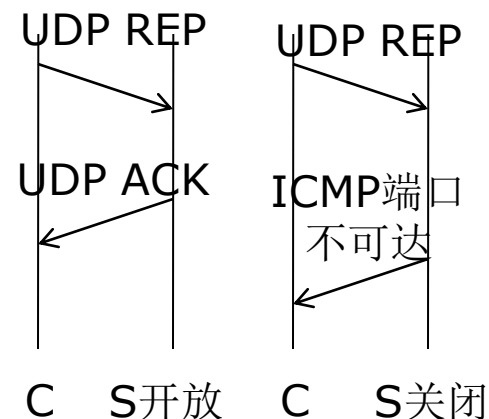
□ 如何达成扫描目的

- 开放端口：标准**TCP**协议规范，接受这些伪造**TCP**包，丢弃，无任何反馈
- 关闭端口：反馈**RST**包
- **Windows/Cisco**等系统没有遵从规范，开放端口对于伪造**TCP**包也反馈**RST**，这三种方法不适用

UDP端口扫描

□ UDP端口扫描

- 对目标端口发送特殊定制的**UDP**数据报文
- 开放端口: **UDP**反馈
- 关闭端口: **ICMP port unreachable**报文



□ UDP端口扫描工具

- **UNIX:** `udp_scan`, `nmap -sU`,
`nc -u -v -z -w2 HOST PORT_LIST`
- **Win32:** `WUPS`, `ScanLine`

扫描软件-nmap*

□ nmap (Network Mapper)

■ 作者: **Fyodor (insecure.org)**

Nmap命令行选项	功能说明
nmap -sT	TCP Connect()扫描
nmap -sS	TCP SYN扫描
nmap -sF	FIN端口扫描
nmap -sN	NULL端口扫描
nmap -sA	ACK端口扫描
nmap -sX	圣诞树端口扫描
nmap -sU	UDP端口扫描

□ nmap图形化支持: **nmap FE, Zenmap**

□ *需重点掌握的工具



Nmap进行端口扫描示例

```
root@administrator-desktop:~# nmap -sS 173.**.*.188  
Starting Nmap 5.00 ( http://nmap.org ) at 2010-7-22 23:51 CST  
Interesting ports on localhost (172.**.*.188):  
Not shown: 998 closed ports  
MAC Address:00:50:**.*.*:D1 (VMWare)  
Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	Ssh
23/tcp	open	telnet
25/tcp	open	Smtp
53/tcp	open	Domain
80/tcp	open	http
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3306/tcp	open	Mysql
5432/tcp	open	Postgresql
8009/tcp	open	ajp13
8180/tcp	open	Unknown

```
MAC Address:00:50:**.*.*:D1 (VMWare)  
Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
```



端口扫描防范措施

- 任何攻击技术都是双刃剑
 - 网络管理员也可利用端口扫描确定开放必要服务
- 端口扫描的监测
 - 网络入侵检测系统: **Snort**中的**portscan**检测插件
 - 系统扫描检测工具: **scanlogd, PortSentry, Genius**
- 端口扫描的预防
 - 开启防火墙
 - 类**UNIX**: **netfilter/IPTables**, **Win32**: 个人防火墙
 - 禁用所有不必要的服务,尽可能减少暴露面(进一步的受攻击面)
 - 类**UNIX**: **/etc/inetd.conf**, **Win32**: 控制面板/服务

系统类型探查

- 系统类型探查：探查活跃主机的系统及开放网络服务的类型
 - 目标主机上运行着何种类型什么版本的操作系统
 - 各个开放端口上监听的是哪些网络服务
- 目的
 - 为更为深入的情报信息收集，真正实施攻击做好准备
 - 如远程渗透攻击需了解目标系统操作系统类型，并配置

技术类型	技术目标与特性	经典工具
操作系统主动探测技术	主动与目标系统通信探测目标系统操作系统	nmap -O, queso
操作系统被动辨识技术	被动监测网络通信以识别目标系统操作系统	P0f, siphon
网络服务主动探测技术	主动与目标系统通信探测目标网络中开放端口上绑定的网络应用服务类型和版本	nmap -sV,
网络服务被动辨识技术	被动监测网络通信以识别目标网络中开放端口上绑定的网络应用服务类型和版本	PADS



操作系统类型探查

- 操作系统类型探查(**OS Identification**)
 - 通过各种不同操作系统类型和版本实现机制上的差异
 - 通过特定方法以确定目标主机所安装的操作系统类型和版本的技术手段
 - 明确操作系统类型和版本是进一步进行安全漏洞发现和渗透攻击的必要前提
- 不同操作系统类型和版本的差异性
 - 协议栈实现差异—协议栈指纹鉴别
 - 开放端口的差异—端口扫描
 - 应用服务的差异—旗标攫取
- 辨识方式
 - 主动—操作系统主动探测技术
 - 被动—被动操作系统识别技术



操作系统主动探测

□ 操作系统主动探测技术

- 端口扫描
- 应用服务旗标攫取
- 主动协议栈指纹鉴别

□ 主动协议栈指纹鉴别

- **Fyodor, Phrack, Remote OS detection via TCP/IP Stack Finger-Printing, 1998.**
- 鉴别项: **FIN, BOGUS flag, ISN采样, DF位, TCP初始窗口大小, ACK值, ICMP出错消息抑制, ICMP消息引用, ICMP出错消息回射完整性, TOS, 重叠分片处理, TCP选项**
- **nmap -O选项, qeuso, Xprobe**



Nmap进行操作系统探测示例

```
[root@icstMySQL ~]# nmap -O 192.168.68.253
```

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2008-10-10 16:05 CST
```

```
Interesting ports on 192.168.68.253:
```

```
(The 1664 ports scanned but not shown below are in state: closed)
```

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

111/tcp	open	rpcbind
---------	------	---------

992/tcp	open	telnets
---------	------	---------

2008/tcp	open	conf
----------	------	------

3306/tcp	open	mysql
----------	------	-------

3389/tcp	filtered	ms-term-serv
----------	----------	--------------

```
MAC Address: 00:90:0B:04:F8:96 (Lanner Electronics)
```

```
Device type: general purpose
```

```
Running: Linux 2.4.X|2.5.X|2.6.X
```

```
OS details: Linux 2.4.7 - 2.6.11
```

```
Uptime 27.368 days (since Sat Sep 13 07:15:51 2008)
```

```
Nmap finished: 1 IP address (1 host up) scanned in 5.038 seconds
```



被动操作系统识别

□ 被动操作系统识别技术

- 流量监听(开放端口): **tcpdump**, ...
- 被动应用服务识别: **PADS**
- 被动协议栈指纹鉴别: **siphon**, **p0f**

□ 被动协议栈指纹鉴别

- **Lance Spitzner, Passive fingerprinting**
- 四个常用特征: **TTL, Window Size, DF, TOS**
- **P0f v2: p0f.fp,**
 - ***www:ttt:D:ss:000...:QQ:OS:Details***
 - ***WWS:TTL:DF:Syn pkt size:option,order,...quirks***
 - ***OS genre, OS description***



P0f进行被动操作系统识别示例

```
root@bt:~# p0f 'src host 172.**.**.188 or dst host 172.**.**.188'
```

p0f - passive os fingerprinting utility, version 2.0.8

(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>

p0f: listening (SYN) on 'eth0', 262 sigs (14 generic, cksum 0F1F5CA2), rule: 'src host 172.**.**.188 or dst host 172.**.**.188'.

172.**.**.188:42228 - **Linux 2.6 (newer, 1)** [high throughput] (up: 349 hrs)

-> 172.**.**.178:80 (distance 0, link: ethernet/modem)

172.**.**.188:45090 - Linux 2.6 (newer, 1) [high throughput] (up: 349 hrs)

-> 172.**.**.178:23 (distance 0, link: ethernet/modem)

172.**.**.178:51659 - Linux 2.6 (newer, 2) [high throughput] (up: 140 hrs)

-> 172.**.**.188:80 (distance 0, link: ethernet/modem)



网络服务类型探查

□ 网络服务类型探查

- 确定目标网络中开放端口上绑定的网络应用服务类型 and 版本
- 了解目标系统更丰富信息, 可支持进一步的操作系统辨识和漏洞识别

□ 网络服务主动探测

- 网络服务旗标抓取和探测: **nmap -sV**

□ 网络服务被动识别

- 网络服务特征匹配和识别: **PADS**



Nmap进行网络服务辨识示例

```
root@administrator-desktop:~# nmap -sV 173.***.188
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-7-23 00:09 CST
```

```
Interesting ports on localhost (172.***.188):
```

```
Not shown: 998 closed ports
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	ProFTPD 1.3.1
22/tcp	open	ssh	OpenSSH 4.7p1Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	Postgresql	PostgreSQL DB
8009/tcp	filtered	ajp13	
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

```
MAC Address:00:50:***.***.***:D1 (VMWare)
```

```
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux
```

```
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 22.68 seconds
```



PADS进行网络服务被动辨识示例

```
[root@icstMySQL pads-1.2]# pads
pads - Passive Asset Detection System
v1.2 - 06/17/05
Matt Shelton <matt@mattshelton.com>

[-] Filter: (null)
[-] Listening on interface eth0

[*] Asset Found: IP Address - 192.168.68.241 / MAC Address - 0:90:0B:08:5F:3C
(Lanner Electronics)
[*] Asset Found: Port - 3306 / Host - 192.168.68.125 / Service - unknown / App
lication - unknown
[*] Asset Found: Port - 22 / Host - 192.168.68.125 / Service - ssh / Applicati
on - OpenSSH 3.9p1 (Protocol 1.99)
[*] Asset Found: IP Address - 192.168.68.125 / MAC Address - 0:90:0B:04:F8:92
(Lanner Electronics)
[*] Asset Found: IP Address - 192.168.68.243 / MAC Address - 0:90:0B:0A:21:86
(Lanner Electronics)
[*] Asset Found: IP Address - 192.168.68.242 / MAC Address - 0:90:0B:09:7D:34
(Lanner Electronics)
[*] Asset Found: IP Address - 192.168.68.14 / MAC Address - 0:E0:4C:B3:13:5A (
Realtek Semiconductor Corp.)
```



系统类型探查防范措施

- 并没有太多好办法
- 检测
 - 端口扫描监测工具
 - 对被动式静默监听并辨识系统类型行为则基本无能为力
- 挫败系统类型探查活动的防御机制也很难
- “不出声就不会被发现”这一古老格言并不适用于网络攻防领域
- 应立足于
 - 即使攻击者探查出了操作系统和网络服务类型，也不能轻易的攻破这道“坚固的防线”



什么是漏洞扫描？

□ 漏洞

- **Security Vulnerability**，安全脆弱性
- 一般认为，漏洞是指硬件、软件或策略上存在的的安全缺陷，从而使得攻击者能够在未授权的情况下访问、控制系统。

□ 漏洞扫描

- 检查系统是否存在已公布安全漏洞，从而易于遭受网络攻击的技术。
-



漏洞的不可避免

□ 系统设计缺陷

- **Internet**从设计时就缺乏安全的总体架构和设计
- **TCP/IP**中的三阶段握手

□ 软件源代码的急剧膨胀

- **Windows 95 1500**万行 **Windows 98 1800**万行
- **Windows XP 3500**万行 **Windows Vista 5000**万行
- **Linux** 内核**200**万行

□ 软件实现的缺陷

- 微软开发人员的单体测试缺陷从超过**25**个缺陷/千行代码显著降低到**7**个缺陷/千行代码
-



漏洞扫描

□ 漏洞扫描技术

- 检查系统是否存在已公布安全漏洞，从而易于遭受网络攻击的技术。
- 双刃剑
 - 网络管理员用来检查系统安全性，渗透测试团队(**Red Team**)用于安全评估。
 - 攻击者用来列出最可能成功的攻击方法，提高攻击效率。

□ 已发布安全漏洞数据库

- 业界标准漏洞命名库**CVE** <http://cve.mitre.org>
- 微软安全漏洞公告**MSxx-xxx**
<http://www.microsoft.com/china/technet/security/current.msp>
- **SecurityFocus BID**
<http://www.securityfocus.com/bid>
- **National Vulnerability Database: NVD**
<http://nvd.nist.gov/>



漏洞扫描软件

❑ ISS (Internet Security Scanner)

- 1993年: 第一个漏洞扫描软件, 商业
- 2006年被IBM以16亿美元收购

❑ SATAN/SAINT

- 1995年: Dan Farmer
- 第一个公开发布的漏洞扫描软件, 引发媒体负面报导

❑ Nessus*

- 目前最优秀的共享漏洞扫描软件
- 1998-: Renaud Deraison, Nessus v2.x 开源
- 2005-: Tenable Network Security, Nessus v3.x, v4.x, freeware, plugin license



Nessus

□ 客户端/服务器模式

- 服务器端: **nessesd (Tcp 1241)**
- 客户端: **nessus -q** (命令行客户端), **nessus**(UNIX图形客户端), **Nessus Client**(Win32客户端)

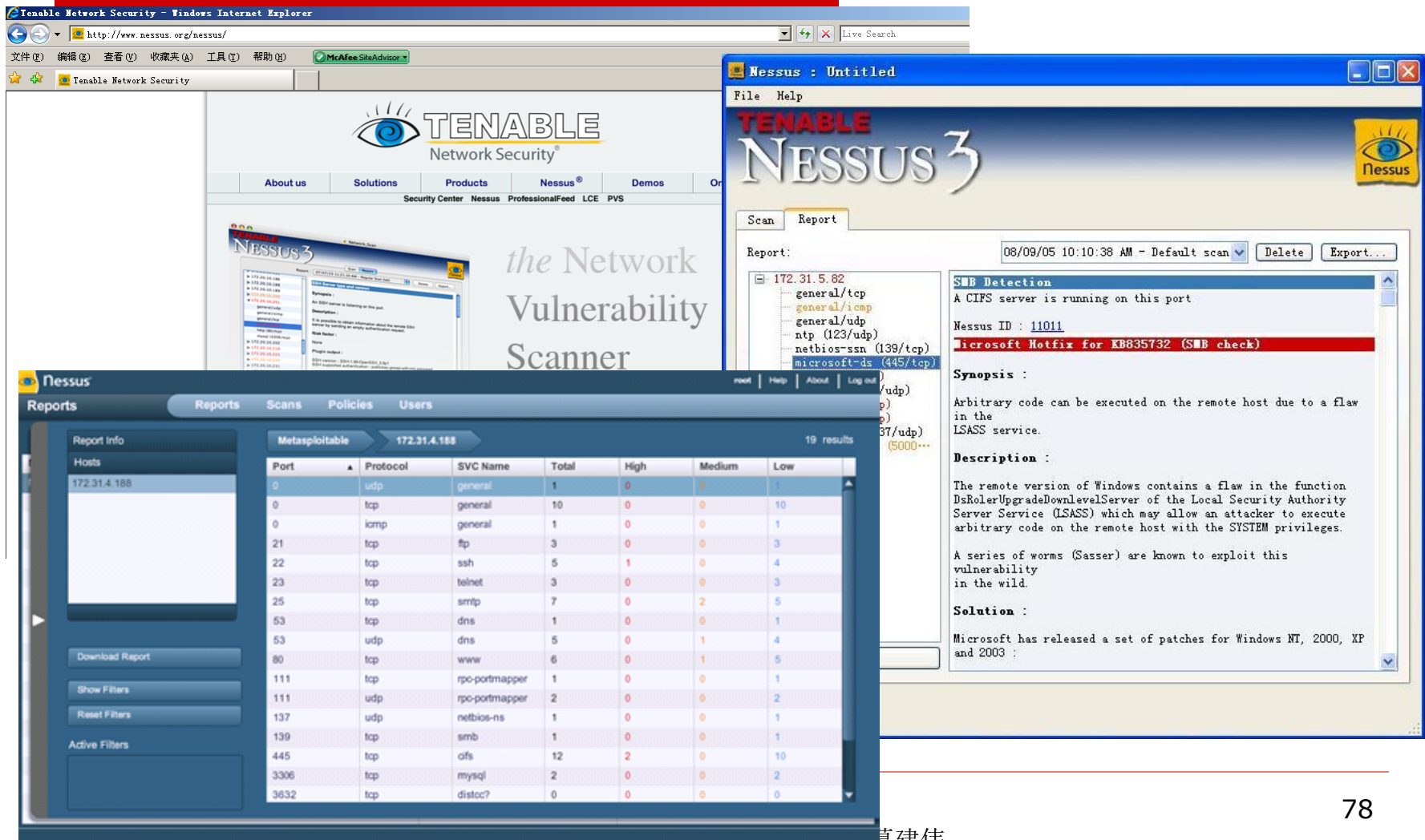
□ 框架/插件模式

- **NASL语言(Nessus Attack Scripting Language)**
- 安全漏洞扫描插件: 使用**NASL**语言容易编写并集成至**Nessus**框架中
- 插件间可互相依赖和协同工作(端口探测—漏洞扫描插件)

□ 多种报告方式:

- 文本/**LaTeX/HTML/DHTML/XML/SQL**等

Nessus



Tenable Network Security - Windows Internet Explorer

http://www.nessus.org/nessus/

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H) McAfee SiteAdvisor

Tenable Network Security

TENABLE
Network Security®

About us Solutions Products **Nessus®** Demos Or

Security Center Nessus ProfessionalFeed LCE PVS

NESSUS 3

the Network Vulnerability Scanner

Nessus : Untitled

File Help

TENABLE
NESSUS 3

Scan Report

Report: 08/09/05 10:10:38 AM - Default scan Delete Export...

172.31.5.82

- general/tcp
- general/icmp
- general/udp
- ntp (123/udp)
- netbios-ssn (139/tcp)
- microsoft-ds (445/tcp)

SMB Detection

A CIFS server is running on this port

Nessus ID : **11011**

Microsoft Hotfix for KB835732 (SMB check)

Synopsis :

Arbitrary code can be executed on the remote host due to a flaw in the LSASS service.

Description :

The remote version of Windows contains a flaw in the function DsRolerUpgradeDownlevelServer of the Local Security Authority Server Service (LSASS) which may allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.

A series of worms (Sasser) are known to exploit this vulnerability in the wild.

Solution :

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 :

Reports

Report Info

Hosts

172.31.4.188

Download Report

Show Filters

Reset Filters

Active Filters

Metasploitable 172.31.4.188 19 results

Port	Protocol	SVC Name	Total	High	Medium	Low
0	udp	general	1	0	0	1
0	tcp	general	10	0	0	10
0	icmp	general	1	0	0	1
21	tcp	ftp	3	0	0	3
22	tcp	ssh	5	1	0	4
23	tcp	telnet	3	0	0	3
25	tcp	smtp	7	0	2	5
53	tcp	dns	1	0	0	1
53	udp	dns	5	0	1	4
80	tcp	www	6	0	1	5
111	tcp	rpc-portmapper	1	0	0	1
111	udp	rpc-portmapper	2	0	0	2
137	udp	netbios-ns	1	0	0	1
139	tcp	smb	1	0	0	1
445	tcp	cifs	12	2	0	10
3306	tcp	mysql	2	0	0	2
3632	tcp	distcc?	0	0	0	0

Nessus使用演示



国内的商业漏洞扫描软件

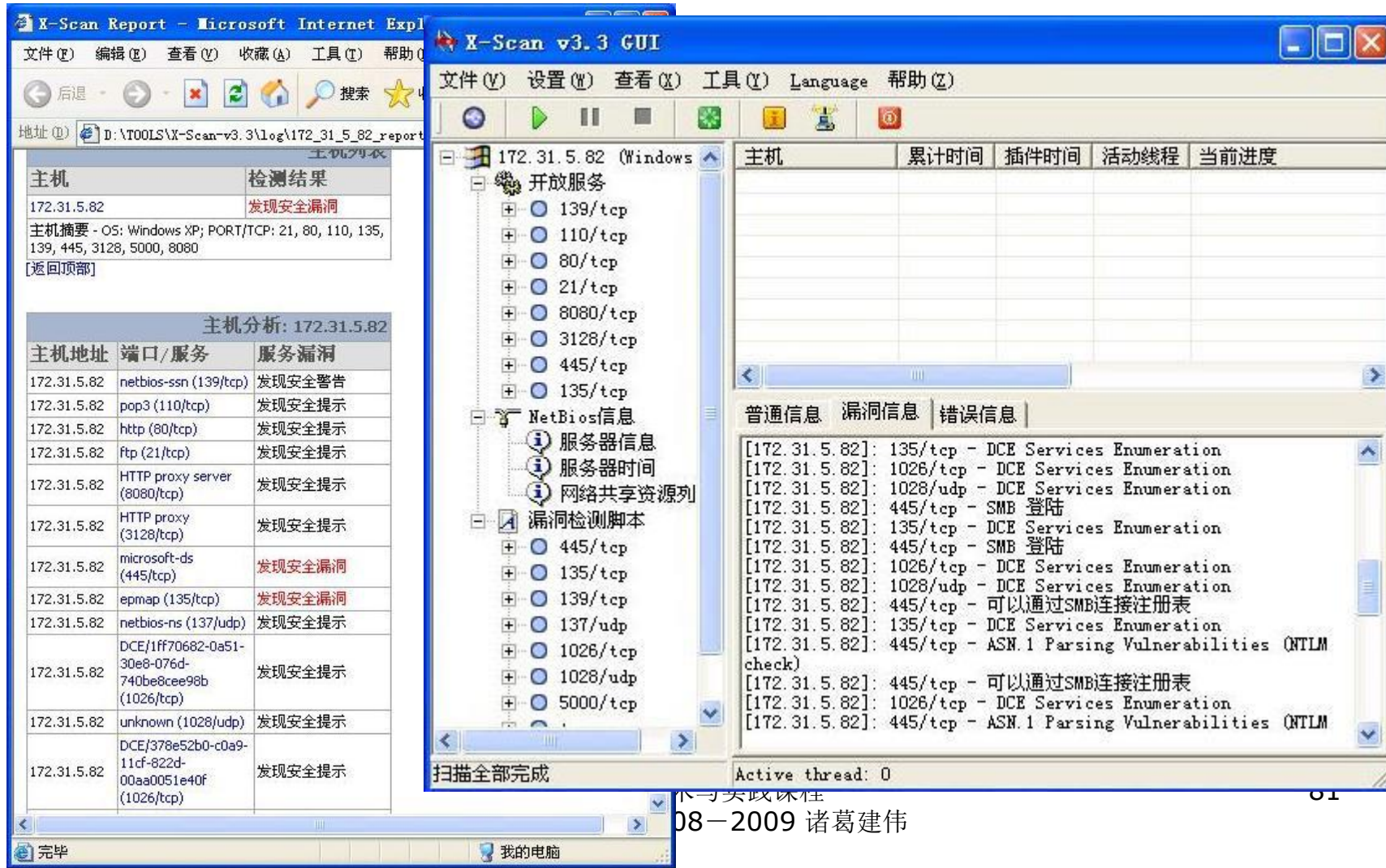
□ 开源软件

- **Xscan***: “冰河” 黄鑫**2001**年开始开发
 - **2005年v3.3**之后无更新
 - 兼容**Nessus**的**NASL**语言开发插件

□ 国内厂商

- 绿盟: “极光”
- 启明星辰: “天镜”
- 方正、中软、东软...

XScan



X-Scan v3.3 GUI

文件(V) 设置(S) 查看(V) 工具(T) Language 帮助(H)

172.31.5.82 (Windows)

- 开放服务
 - 139/tcp
 - 110/tcp
 - 80/tcp
 - 21/tcp
 - 8080/tcp
 - 3128/tcp
 - 445/tcp
 - 135/tcp
- NetBios信息
 - 服务器信息
 - 服务器时间
 - 网络共享资源列
- 漏洞检测脚本
 - 445/tcp
 - 135/tcp
 - 139/tcp
 - 137/udp
 - 1026/tcp
 - 1028/udp
 - 5000/tcp

扫描全部完成 Active thread: 0

主机	检测结果
172.31.5.82	发现安全漏洞

主机摘要 - OS: Windows XP; PORT/TCP: 21, 80, 110, 135, 139, 445, 3128, 5000, 8080
[返回顶部]

主机分析: 172.31.5.82

主机地址	端口/服务	服务漏洞
172.31.5.82	netbios-ssn (139/tcp)	发现安全警告
172.31.5.82	pop3 (110/tcp)	发现安全提示
172.31.5.82	http (80/tcp)	发现安全提示
172.31.5.82	ftp (21/tcp)	发现安全提示
172.31.5.82	HTTP proxy server (8080/tcp)	发现安全提示
172.31.5.82	HTTP proxy (3128/tcp)	发现安全提示
172.31.5.82	microsoft-ds (445/tcp)	发现安全漏洞
172.31.5.82	epmap (135/tcp)	发现安全漏洞
172.31.5.82	netbios-ns (137/udp)	发现安全提示
172.31.5.82	DCE/1ff70682-0a51-30e8-076d-740be8cee98b (1026/tcp)	发现安全提示
172.31.5.82	unknown (1028/udp)	发现安全提示
172.31.5.82	DCE/378e52b0-c0a9-11cf-822d-00aa0051e40f (1026/tcp)	发现安全提示

普通信息 漏洞信息 错误信息

```
[172.31.5.82]: 135/tcp - DCE Services Enumeration
[172.31.5.82]: 1026/tcp - DCE Services Enumeration
[172.31.5.82]: 1028/udp - DCE Services Enumeration
[172.31.5.82]: 445/tcp - SMB 登陆
[172.31.5.82]: 135/tcp - DCE Services Enumeration
[172.31.5.82]: 445/tcp - SMB 登陆
[172.31.5.82]: 1026/tcp - DCE Services Enumeration
[172.31.5.82]: 1028/udp - DCE Services Enumeration
[172.31.5.82]: 445/tcp - 可以通过SMB连接注册表
[172.31.5.82]: 135/tcp - DCE Services Enumeration
[172.31.5.82]: 445/tcp - ASN.1 Parsing Vulnerabilities (NTLM check)
[172.31.5.82]: 445/tcp - 可以通过SMB连接注册表
[172.31.5.82]: 1026/tcp - DCE Services Enumeration
[172.31.5.82]: 445/tcp - ASN.1 Parsing Vulnerabilities (NTLM
```

08-2009 诸葛建伟



漏洞扫描防范措施

□ 最简单对策:

- 假设黑客会使用漏洞扫描来发现目标网络弱点，那你必须在黑客之前扫描漏洞
- 补丁自动更新和分发：修补漏洞

□ 联邦桌面核心配置计划(**FDCC**)

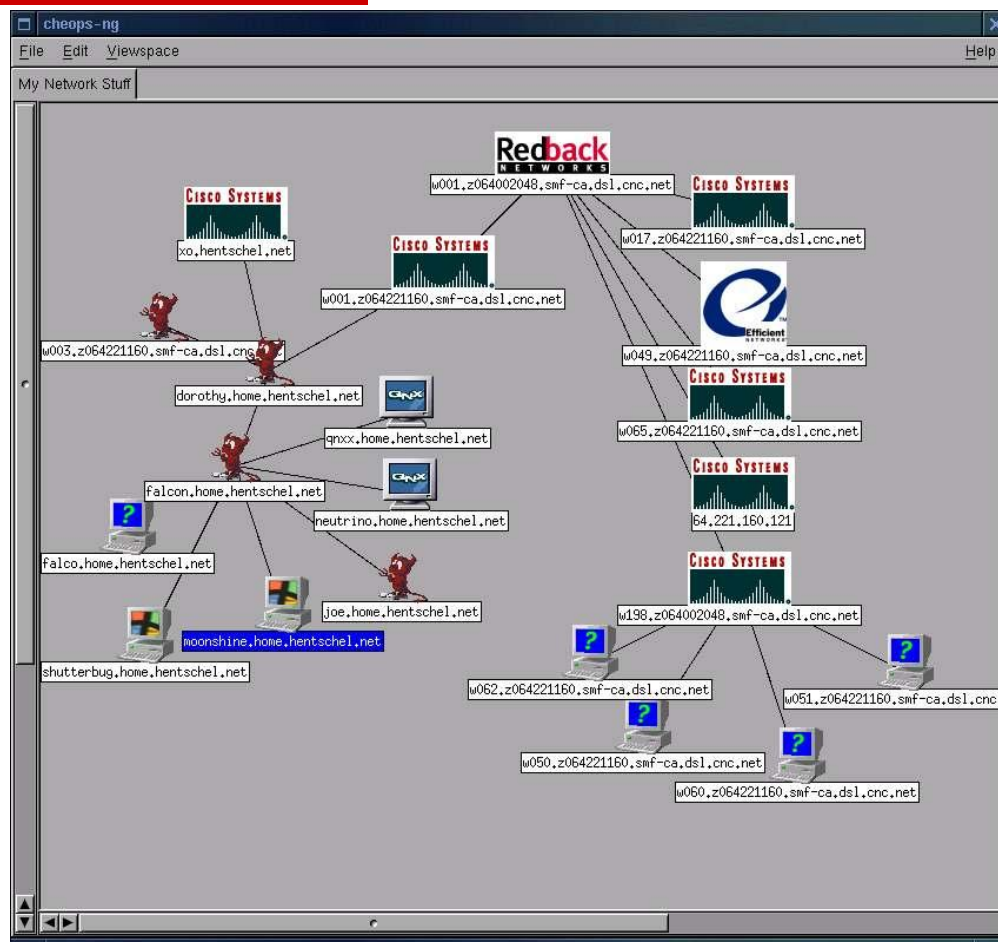
- 确保桌面计算机的安全漏洞及补丁自动管理
- 中国**2010**年才开始政务终端安全配置(**CGDCC**)标准的发展

□ 检测和防御漏洞扫描行为

- 网络入侵检测系统: **Snort**
- 仔细审查防火墙配置规则

完整解决方案-自动化侦察工具

- 自动化侦察工具
 - HP OpenView
 - Cheops
 - Cheops-ng
 - tkined





内容

1. 网络基础知识
2. 网络信息采集技术概述
3. 网络踩点技术
4. 课堂实践：DNS与IP查询
5. 网络扫描技术
6. 课堂实践：nmap扫描
7. 作业3—搜索自己的互联网足迹/网络扫描实验



课堂实践：Nmap

- 任务：使用**Nmap**开源软件对靶机环境进行扫描，回答如下问题并给出操作命令：
 - 靶机**IP**地址是否活跃？
 - 靶机开放了那些**TCP**和**UDP**端口？
 - 靶机安装了什么操作系统？版本是多少？
 - 靶机上安装了哪些网络服务？



内容

1. 网络基础知识
2. 网络信息采集技术概述
3. 网络踩点技术
4. 课堂实践：DNS与IP查询
5. 网络扫描技术
6. 课堂实践：nmap扫描
7. 作业3—搜索自己的互联网足迹/网络扫描/Nessus扫描实验



作业3 – 个人作业

- **3.1** 通过搜索引擎搜索自己在因特网上的足迹，并确认是否存在隐私和敏感信息泄露问题，如是，提出解决方法。（注，不要在提交作业中泄漏个人隐私☺）
- **3.2** 使用**Nmap**扫描某台靶机，并给出靶机环境的配置情况，撰写实验分析报告。
- **3.3** 使用**Nessus**扫描某台靶机，并给出靶机环境上的网络服务及安全漏洞情况，撰写实验分析报告。

- 提交给助教: **zhanghuilin@icst.pku.edu.cn**
- **Deadline: 10月20日**

Thanks

诸葛建伟

zhugejianwei@icst.pku.edu.cn