网 络 安 全

——信息收集

杭州师范大学信息科学与技术学院

刘雪娇　邮箱：liuxuejiao0406@163.com

本章节要求

- 了解和掌握信息收集的相关概念
- 关注常见信息收集的方法
- 掌握网络扫描的相关知识点
- 具有信息收集的基本实践能力

目录

引言

预攻击

目的：
收集信息，进行进一步攻击决策

内容：
获取域名及IP分布
获取拓扑及OS等
获得端口和服务
获得应用系统的情况
跟踪新漏洞发布

攻击

目的：
进行攻击，获得系统的一定权限

内容：
获取远程权限
进入远程系统
提升本地权限
进一步扩展权限
进行实质性操作

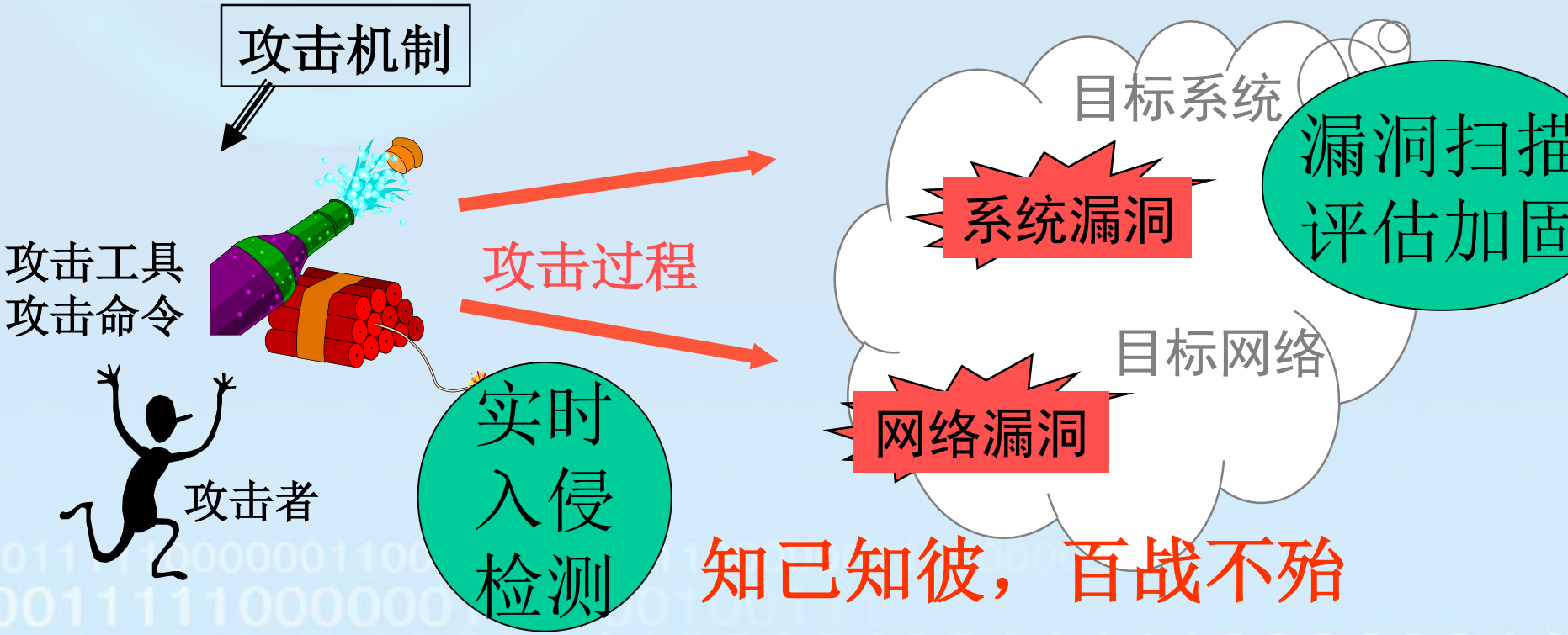
后攻击

目的：
消除痕迹，长期维持一定的权限

内容：
植入后门木马
删除日志
修补明显的漏洞
进一步渗透扩展

信息收集

- **信息收集技术是一把双刃剑**
  - ✓ 黑客在攻击之前需要收集信息，才能实施有效的攻击
  - ✓ 安全管理员用信息收集技术来发现系统的弱点并进行修补



信息收集的必要性

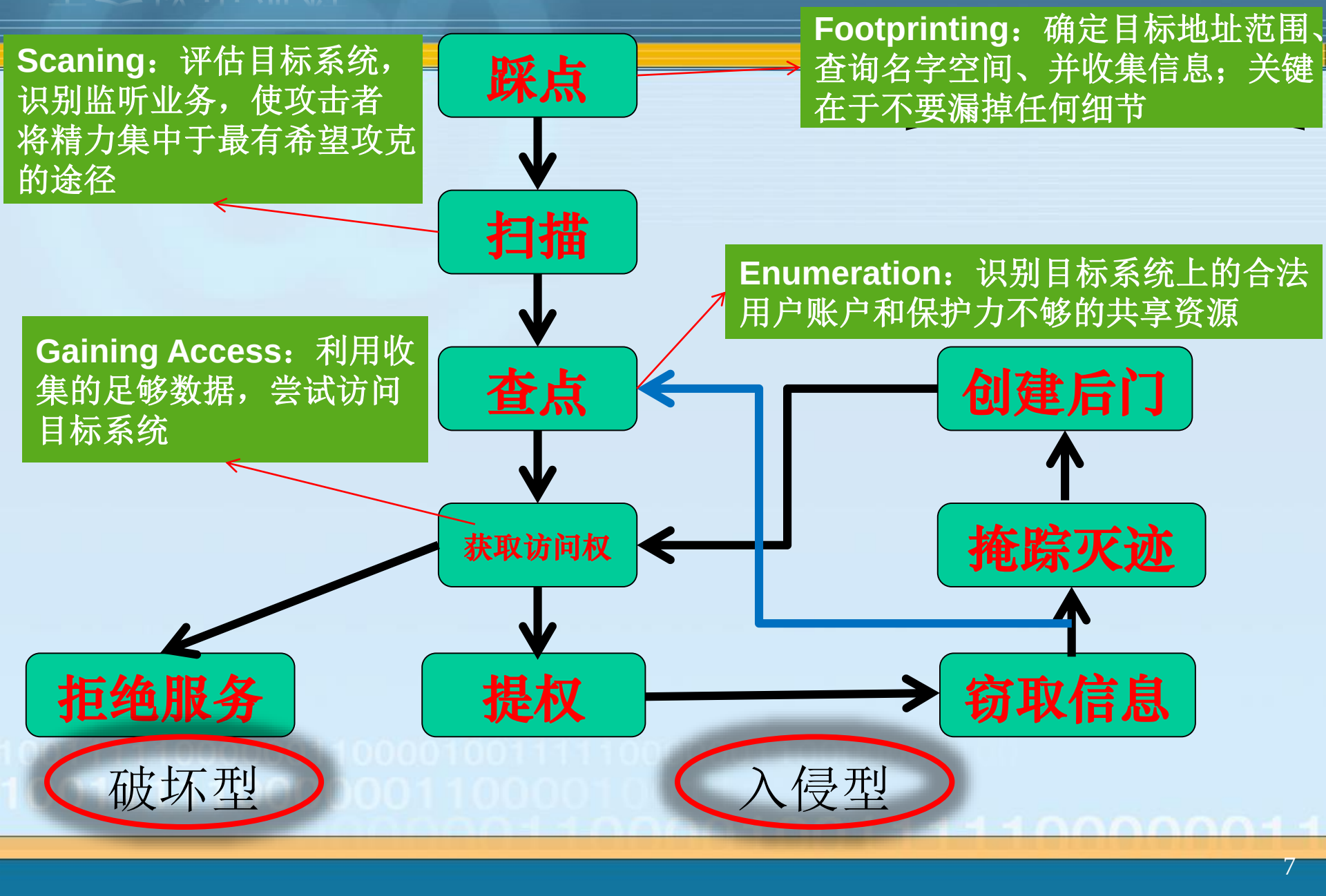
- “知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼，不知己，每战必殆。”
  ——《孙子·谋攻篇》

- 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

黑客攻击流程


Footprinting：确定目标地址范围、查询名字空间、并收集信息；关键在于不要漏掉任何细节
Scaning：评估目标系统，识别监听业务，使攻击者将精力集中于最有希望攻克的途径
Enumeration：识别目标系统上的合法用户账户和保护力不够的共享资源
Gaining Access：利用收集的足够数据，尝试访问目标系统
踩点
扫描
查点
获取访问权
提权
拒绝服务
创建后门
掩踪灭迹
窃取信息
破坏型
入侵型

信息收集

信息收集（Information Gathering）是指对目标主机、目标网络、相关的系统管理人员进行非公开的检测，全面收集目标系统的信息。信息收集是信息得以利用的第一步，也是关键的一步。

信息收集是一个综合的过程

从一些社会信息入手

找到网络地址范围

找到开放端口和入口点

找到系统的制造商和版本

……

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” ：Zoomeye(https://www.zoomeye.org/(钟馗之眼)
  - 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

- ✓ 攻追查入侵者的身份、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

信息收集技术

网络踩点
Footprinting

网络扫描与探测
Scanning

网络查点
Enumeration

➢ **网络踩点**

- ✓ Web搜索与挖掘(Google Hacking,Whois等）攻击
- ✓ DNS与IP查询（Ping，Traceroute等）
- ✓ Web指纹识别

➢ **网络扫描与探测**

- ✓ 主机扫描
- ✓ 端口扫描
- ✓ 系统类型识别
- ✓ 漏洞扫描

➢ **网络查点**

- ✓ 旗标抓取
- ✓ 网络服务查点

网络踩点技术

- **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**
  - 收集网络信息（域名、内网域名、网络划分、IP地址、所使用的网络协议、VPN接入点）
  - 收集系统信息（用户名或组名、路由表、操作系统类型、系统密码、系统架构）
  - 收集组织单位信息（人员信息、组织网络、地址及电话、组织背景、最新动态）

踩点


https://vpn.cumt.edu.cn/dana-na/auth/url_default/welcome.cgi
中国矿业大学VPN系统
中国矿业大学
CHINA UNIVERSITY OF MINING AND TECHNOLOGY
Juniper Netscreen SS
L VPN
用户登录 / LOGIN
用户名:
密 码:
登 录

基于搜索引擎的信息探测

- Google Hacking主要用到google、baidu、bing等搜索引擎的搜索技巧。

语法	作用	例子
intitle	搜索标题中包含指定关键字的页面	
inurl	搜索URL地址中包含指定关键字的网页	inurl:login
site	在指定的站点内搜索	site: hznu.edu.cn 管理 登录
filetype	搜索指定类型的文件（如doc、pdf、ppt）	filetype:xls 身份证 手机
link	返回所有链接到某个URL地址的网页	
related	搜索与指定网站有关联的主页	
cache	指明在Google缓存中搜索	
intext	搜索正文中出现指定关键字的页面	intext:index of passwd

基于Whois数据库的信息探测

- Whois
  - ✓为Internet提供目录服务，包括名字、通讯地址、电话号码、电子邮箱、IP地址等信息
- Client/Server结构
  - ✓Client端
    - 发出请求，接受结果，并按格式显示到客户屏幕上
  - ✓Server端
    - 建立数据库，接受注册请求，提供在线查询服务
- 客户程序
  - ✓UNIX系统自带whois程序
  - ✓Windows也有一些工具
  - ✓直接通过Web查询

```
ubuntu@VM-2-129-ubuntu:~$ whois nt.cn
Domain Name: nt.cn
ROID: 20030311s10001s00033951-cn
Domain Status: ok
Registrant ID: hc1994196330073
Registrant: 北京牛谈互联网服务有限公司
Registrant Contact Email: jiaxing.sun@chinanx.com
Sponsoring Registrar: 阿里云计算有限公司（万网）
Name Server: dns7.hichina.com
Name Server: dns8.hichina.com
Registration Time: 2003-03-17 12:20:05
Expiration Time: 2026-03-17 12:48:36
DNSSEC: unsigned
ubuntu@VM-2-129-ubuntu:~$
```

http://www.internic.net/wh

站长之家http://whois.chinaz.com

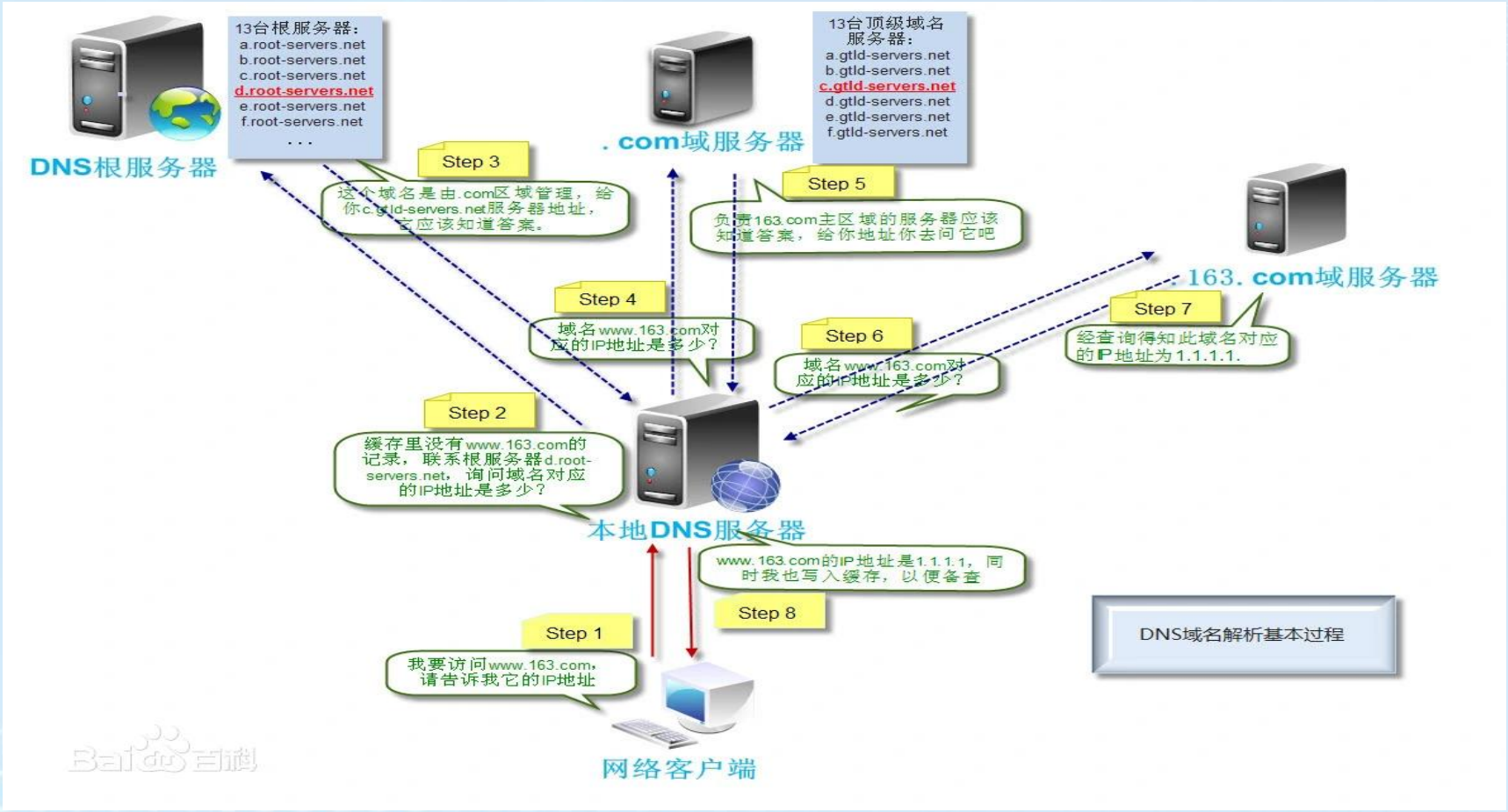
阿里云域名信息查询https://whois.aliyun.com

利用DNS服务器的域名信息探测技术

- 关于DNS
  - ✓ 是一个全球分布式数据库，对于每一个DNS节点，包含有该节点所在的机器的信息、邮件服务器的信息、主机CPU和操作系统等信息
  - ✓ Nslookup是一个功能强大的客户程序
- 熟悉nslookup，就可以把DNS数据库中的信息挖掘出来
  - ✓ 分两种运行模式
    - 非交互式，通过命令行提交命令
    - 交互式：可以访问DNS数据库中所有开放的信息
- UNIX/LINUX环境下的host命令有类似的功能

DNS域名解析过程

域名解析步骤



利用DNS服务器的域名信息探测技术

- **通过nslookup可以做什么？**
  - ✓区域传送：可以列出DNS节点中所有的配置信息
    - 这是为了主DNS和辅DNS之间同步复制才使用的
  - ✓查看一个域名，根据域名找到该域的域名服务器
  - ✓反向解析，根据IP地址得到域名名称

- **从一台域名服务器可以得到哪些信息？**
  - ✓如果支持区域传送，可以从中获取大量信息
  - ✓否则的话，至少可以发现以下信息
    - 邮件服务器的信息，在实用环境中，邮件服务器往往在防火墙附近，甚至就在同一台机器上
    - 其他，比如ns、www、ftp等，这些机器可能被托管给ISP

利用DNS服务器的域名信息探测技术

- nslookup交互环境中常用命令
  - ✓server，指定DNS服务器
  - ✓set type=XXX，设定查询类型
  - ✓ls，列出记录
  - ✓[domain name，or IP address]

```
snowdeMacBook-Air:~ snow$ nslookup www.baidu.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.baidu.com   canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 36.152.44.96
Name:   www.a.shifen.com
Address: 36.152.44.95

snowdeMacBook-Air:~ snow$ nslookup sec.hdu.edu.cn
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
sec.hdu.edu.cn  canonical name = sec.split.hdu.edu.cn.
Name:   sec.split.hdu.edu.cn
Address: 210.32.34.100
```

Ping

- 发送ICMP Echo消息，等待Echo Reply消息
  - ✓可以确定网络和外部主机的状态
  - ✓可以用来调试网络的软件和硬件
- 每秒发送一个包，显示响应的输出，计算网络来回的时间
- 最后显示统计结果——丢包率

```
C:\Users\pyy0820>ping www.baidu.com

正在 Ping www.a.shifen.com [180.101.49.12] 具有 32 字节的数据:
来自 180.101.49.12 的回复: 字节=32 时间=14ms TTL=51
来自 180.101.49.12 的回复: 字节=32 时间=14ms TTL=51
来自 180.101.49.12 的回复: 字节=32 时间=13ms TTL=51
来自 180.101.49.12 的回复: 字节=32 时间=14ms TTL=51

180.101.49.12 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 13ms，最长 = 14ms，平均 = 13ms

C:\Users\pyy0820>
```

Ping

- Ping有许多命令行参数，可以改变缺省的行为
- 可以用来发现一台主机是否active
- 为什么不能ping成功？
  - ✓ 没有路由，网关设置？
  - ✓ 网卡没有配置正确
  - ✓ 增大timeout值
  - ✓ 被防火墙阻止
  - ……

⑩ “Ping of death”
  - ⑩ 发送特大ping数据包(>65535字节)导致机器崩溃
  - ⑩ 许多老的操作系统都受影响

Traceroute

Traceroute是一种网络故障诊断和获取网络拓扑结构的工具；

Traceroute工具可以跟踪TCP/IP数据包从出发点到目的地所走路径：

- 通过发送小的数据包到目的设备直到返回，来测量耗时，并返回设备的名称和地址；
- 通过向目的地发送不同生存时间(TTL)的ICMP报文，以确定到达目的地的路由。

```
C:\Documents and Settings\Administrator>tracert www.sina.com.cn

Tracing route to www.sina.com.cn [202.108.37.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.102.1
  2    <1 ms    <1 ms     1 ms  162.105.[redacted]
  3    <1 ms    <1 ms    <1 ms  162.105.[redacted]
  4     3 ms     3 ms     2 ms  162.105.[redacted]
  5    <1 ms    <1 ms    <1 ms  pku0.cernet.net [202.112.38.73]
  6    <1 ms    <1 ms    <1 ms  202.112.61.185
  7    <1 ms    <1 ms    <1 ms  202.112.61.158
  8     *        *        *     Request timed out.
  9   383 ms   400 ms   390 ms  219.158.11.113
 10   369 ms   376 ms   374 ms  202.96.12.42
 11   387 ms   397 ms   392 ms  202.106.192.174
 12   403 ms   392 ms   403 ms  210.74.176.158
 13   406 ms   407 ms   402 ms  sina37-34.sina.com.cn [202.108.

Trace complete.
```

CDN

```
C:\Users\ibits>tracert www.163.com

通过最多 30 个跃点跟踪
到 163.xdwscache.ourglb0.com [58.216.21.93] 的路由:

  1     3 ms     3 ms     3 ms  192.168.1.1
  2     4 ms     3 ms     3 ms  192.168.167.1
  3     3 ms     3 ms    11 ms  192.168.253.5
  4     7 ms     3 ms     6 ms  192.168.253.1
  5     6 ms     3 ms     4 ms  172.33.1.5
  6     7 ms     3 ms     3 ms  192.168.200.18
  7     6 ms     9 ms     7 ms  58.218.185.1
  8     9 ms     6 ms     8 ms  61.147.6.197
  9    46 ms    12 ms    13 ms  221.229.146.73
 10    25 ms    15 ms    13 ms  61.160.134.14
 11    13 ms    39 ms    13 ms  61.160.214.74
 12    14 ms    17 ms    19 ms  61.160.244.182
 13    14 ms    14 ms    26 ms  58.216.21.93

跟踪完成。
```

web指纹识别技术

Web指纹识别技术：在web渗透过程中，Web指纹识别是信息收集环节中一个比较重要的步骤，通过一些开源的工具、平台或者手工检测CMS系统是公开的CMS程序还是二次开发至关重要，能准确的获取CMS类型、Web服务组件类型及版本信息可以帮助安全工程师快速有效的去验证已知漏洞。

常见的指纹检测的对象：

（1）CMS信息：比如大汉CMS、织梦、帝国CMS、phpcms、ecshop等；

（2）前端技术：比如HTML5、jquery、bootstrap、pure、ace等；

（3）Web服务器：比如Apache、lighttpd, Nginx, IIS等；

（4）应用服务器：比如Tomcat、Jboss、weblogic、websphere等；

（5）开发语言：比如PHP、Java、Ruby、Python、C#等；

（6）操作系统信息：比如linux、win2k8、win7、kali、centos等；

（7）CDN信息：是否使用CDN，如cloudflare、360cdn、365cyd、yunjiasu等；

（8）WAF信息：是否使用waf，如Topsec、Jiasule、Yundun等；

（9）IP及域名信息：IP和域名注册信息、服务商信息等；

（10）端口信息：有些软件或平台还会探测服务器开放的常见端口。

web指纹识别技术

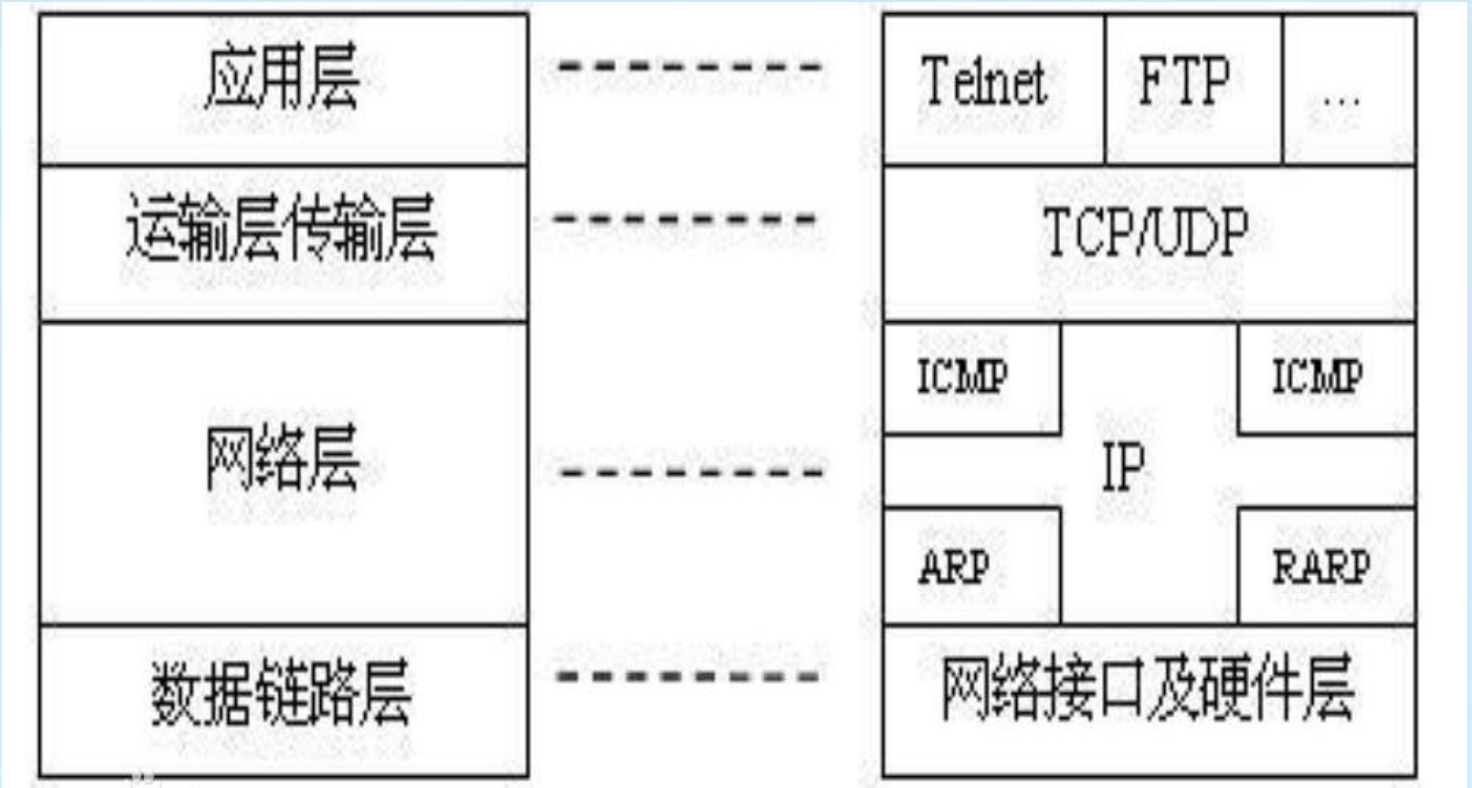
指纹识别工具：

1. 潮汐指纹：http://finger.tidesec.net（要登录）
2. wappalyzer插件
3. whatweb工具
4. CMS识别工具
http://whatweb.bugscaner.com/look
5. 云悉 http://www.yunsee.cn
6. 御剑

网络扫描技术

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

TCP/IP四层结构

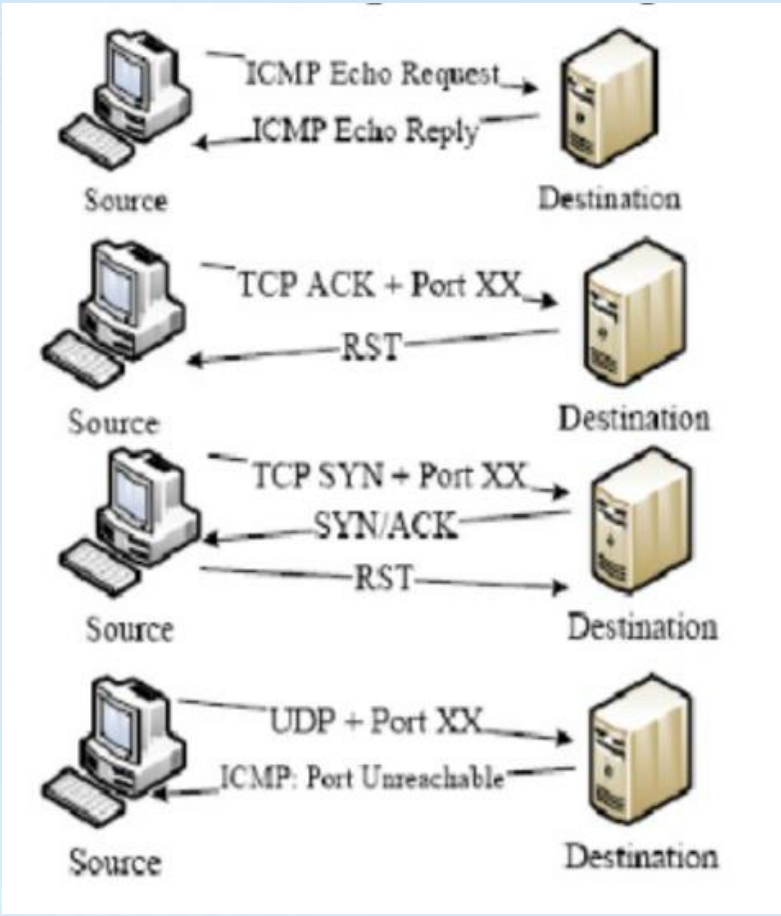

应用层
运输层传输层
网络层
数据链路层
Telnet
FTP
...
TCP/UDP
ICMP
ICMP
IP
ARP
RARP
网络接口及硬件层

主机扫描（ping扫描）

- 主机扫描目的：检查目标主机是否活跃

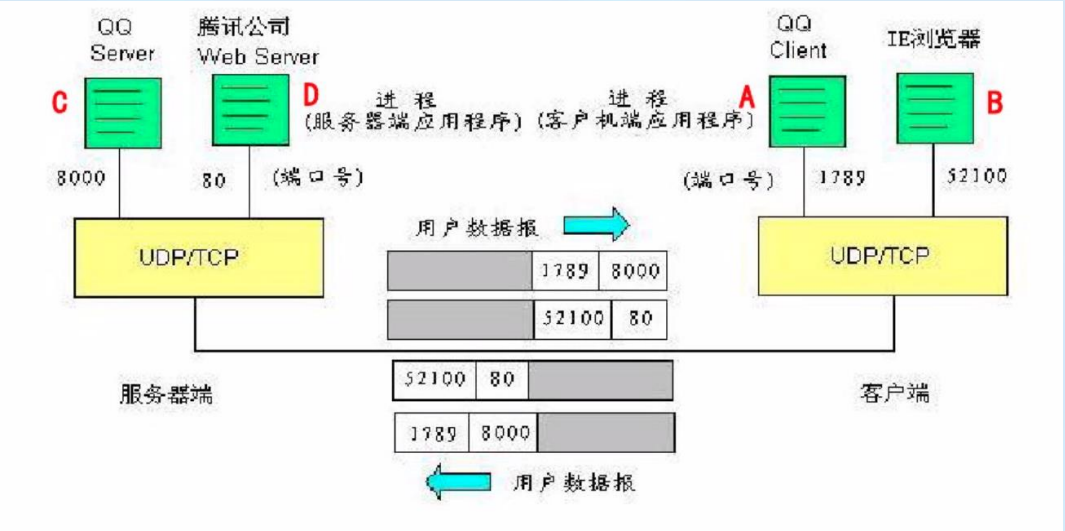
- 主机扫描方式
  - ✓ 传统ICMP Ping扫描
  - ✓ ACK Ping扫描
  - ✓ SYN Ping扫描
  - ✓ UDP Ping扫描：到关闭端口

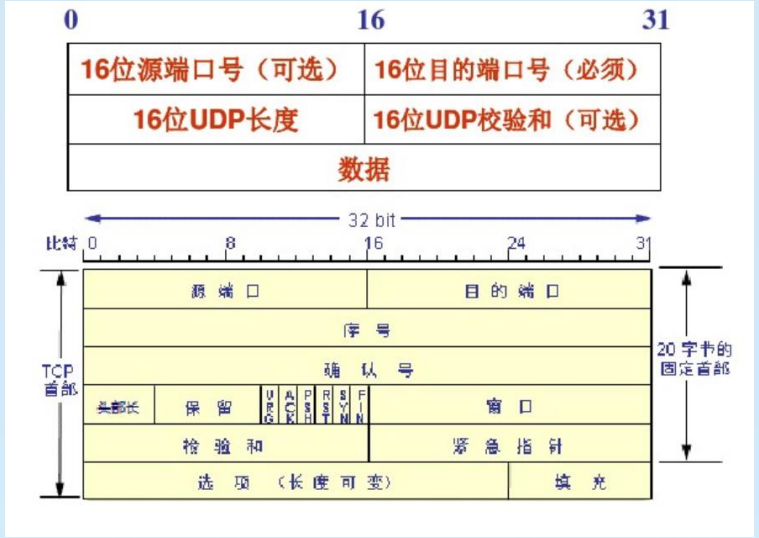
- 主机扫描程序
  - ✓ Ping
  - ✓ Nmap：-sP选项，缺省执行，集合了ICMP/SYN/ACK/UDP Ping功能



端口扫描

端口：端口是传输层协议为了识别同一主机上不同应用程序进程而引入的一个概念。一个端口栈16个比特位，一台主机可供分配的端口数位2^{16-1}=65535个。端口由应用程序申请，操作系统统一管理和分配。





端口扫描

TCP/IP协议规定，用IP地址和端口作为套接字(socket)，代表TCP或UDP通信的一端。端口分为知名(known)端口号和一般端口号，其中知名端口号的数值一般为0~1023,分配给常用的应用服务程序(需要监听IP地址和端口)所固定使用。

端口	应用层协议	说明
53	DNS	域名服务器
69	TFTP	简单文件传输协议
111	RPC	远程过程调用
161	SNMP	简单网络管理协议

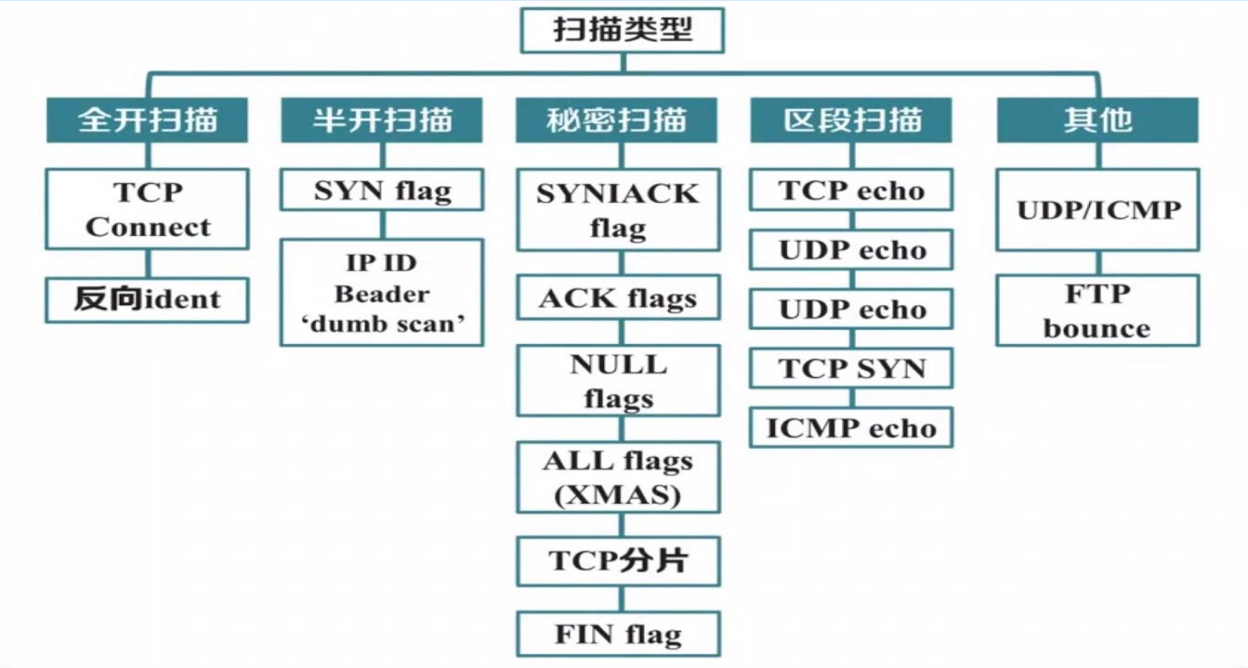
常见的UDP知名端口

端口	应用层协议	说明
20	FTP	文件传输协议（数据连接）
21	FTP	文件传输协议（控制连接）
23	Telnet	远程登录协议
25	SMTP	简单文件传输协议
80	HTTP	超文本传输协议
110	POP3	邮局协议

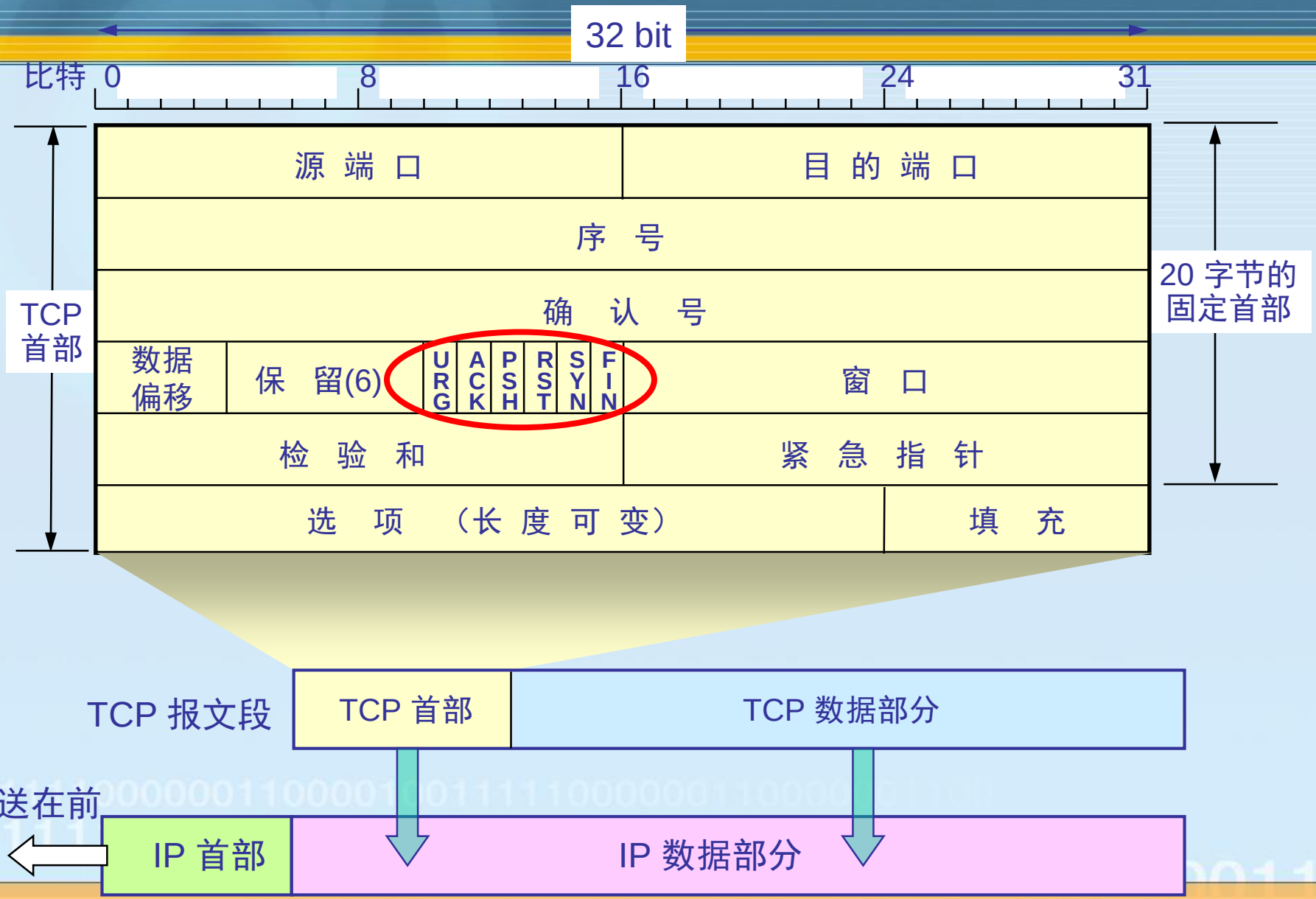
常见的TCP知名端口

端口扫描

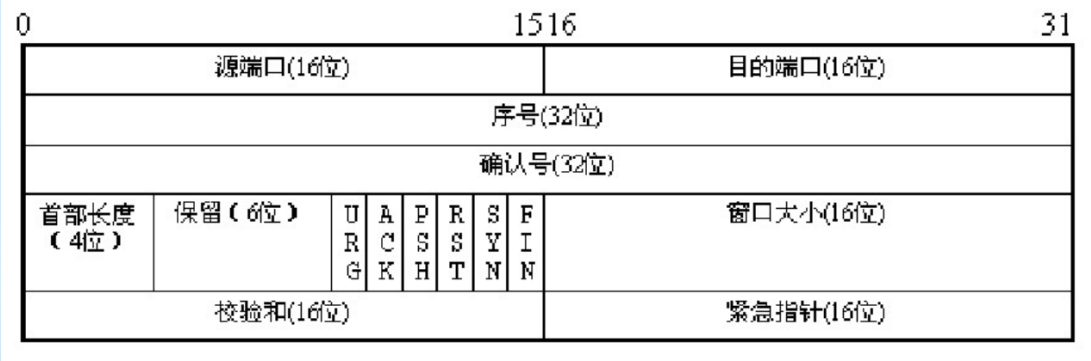
端口扫描的原理：端口扫描是向目标主机的TCP或UDP端口发送探测数据包，随后记录目标主机的响应。通过分析目标主机的响应来判断服务端口是打开还是关闭的，据此推测目标主机端口提供的服务或信息。



端口扫描


32 bit
比特
0
8
16
24
31
源 端 口
目 的 端 口
序 号
确 认 号
数据偏移
保 留(6)
URG
ACK
PSH
RST
SYN
FIN
窗 口
检 验 和
紧 急 指 针
选 项 （长 度 可 变）
填 充
TCP 首部
20 字节的固定首部
TCP 报文段
TCP 首部
TCP 数据部分
发送在前
IP 首部
IP 数据部分

TCP数据报首部标志域



URG：紧急数据标志，指明数据流中已经放置紧急数据，紧急指针有效。

ACK：确认标志，用于对报文的确认。

PSH：推标志，通知接收端尽可能的将数据传递给应用层，在telnet登录时，会使用这个标志。

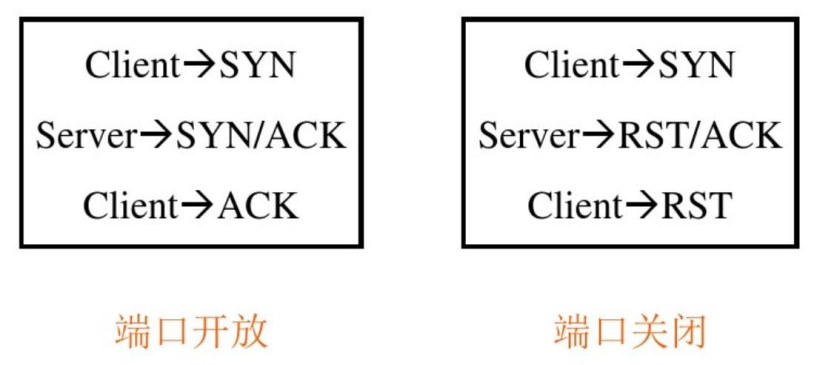
RST：复位标志，用于复位TCP连接。

SYN：同步标志，用于三次握手的建立，提示接收TCP连接的服务端检查序号。

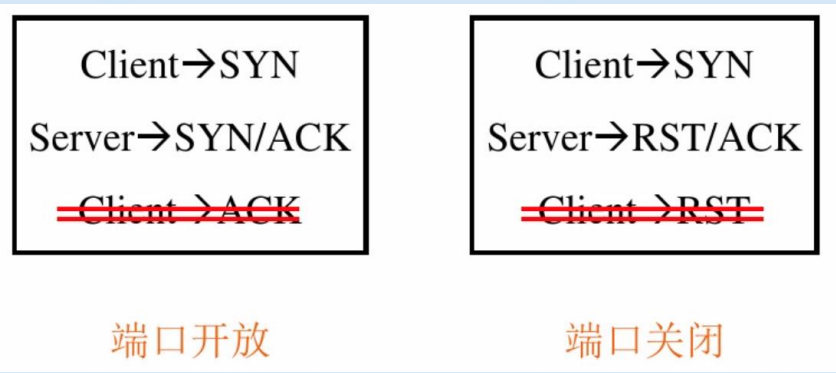
FIN：结束标志，表示发送端已经没有数据再传输了，希望释放连接，但接收端可以继续接收数据。

端口扫描

➢**全连接扫描：**扫描主机通过TCP/IP协议的三次握手与目标主机的指定端口建立一次完整的连接。

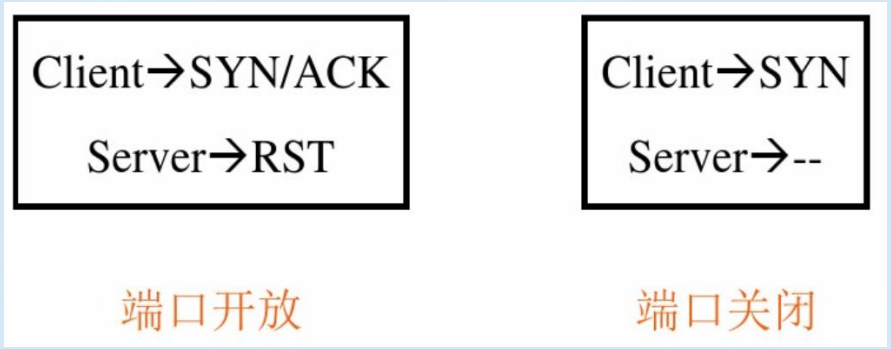


➢**半连接扫描：**只完成了前两次握手，在第三步时，扫描主机中断了本次连接，连接没有完全建立起来，这样的端口扫描中称为半连接扫描。

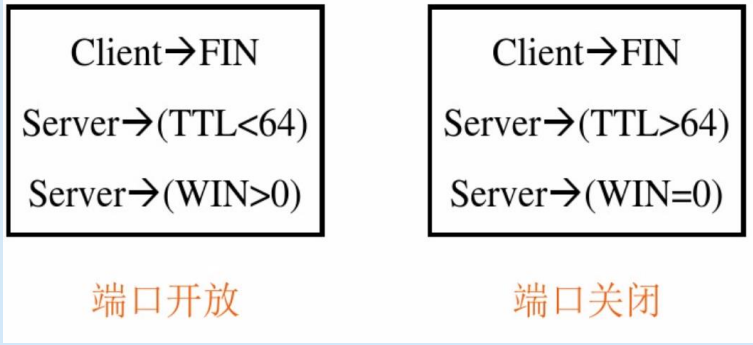


端口扫描

➢**秘密扫描：**没有任何数据的连接进接口，是一种不被审计工具所检测扫描技术。有TCP FIN扫描、TCP ACK扫描、NULL扫描、XMAS扫描、TCP分段扫描和SYN/ACK扫描等。



TCP ACK扫描



TCP FIN扫描

端口扫描

➢**FTP反弹扫描：**FTP服务器允许从一个目录读写数据，则能发送任意的数据到开放的端口。

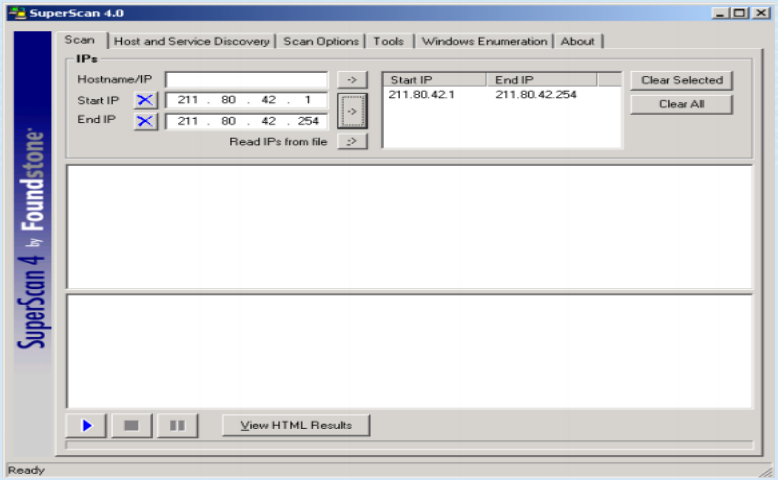
➢**UDP ICMP端口不可到达扫描：**这种扫描使用的是UDP协议。扫描主机发送UDP数据报给目的主机的UDP端口，等待目标端口的端口不可到达的ICMP消息。

优缺点 / 端口扫描技术		优点	缺点
全连接扫描		扫描迅速、准确而且不需要任何权限	易被目标主机发觉而被过滤掉
半连接扫描		一般不会被目标主机记录连接，有利于不被扫描方发现	大部分操作系统下，扫描主机需要构造适用于这种扫描的IP包，而通常情况下，构造自己的SYN数据包必须要有root权限
秘密扫描		能躲避IDS、防火墙、包过滤器和日志审计，从而获取目标端口的开放或关闭的信息。没有包含TCP3次握手协议的任何部分，所以无法被记录下来，比半连接扫描要更为隐蔽	扫描结果的不可靠性增加，而且扫描主机也需要自己构造IP包
其他扫描	FTP反弹攻击	能穿透防火墙，难以跟踪	速度慢且易被代理服务器发现并关闭代理功能
	UDP IC MP端口不可到达扫描	可以扫描非TCP端口，避免了TCP的IDS	由于是基于简单的UDP协议，扫描相对困难，速度慢而且需要root权限

端口扫描

端口扫描探测工具：

- SuperScan：基于Windows平台的图形化工具；探测扫描速度非常快。
- ScanLine：命令行工具。
- Nmap：被称为“扫描器之王”。有Unix和Windows系统中的命令行和图形化各种版本。需要Liapcap库和Winpcap库的支持。能够进行常规扫描、各种高级扫描和操作系统类型鉴别等。




```
> sl -bhpt 1-1024,1433,3389,5900 192.168.1.1-254
```

用法：nmap [选项] <目标地址列表>

```
> nmap -sS -O -P0 www.yahoo.com.cn
Starting nmap 3.81 ( http://www.insecure.org/nmap ) at …
Interesting ports on p14.www.scd.yahoo.com (66.94.230.45):
(The 1661 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap finished: 1 IP address (1 host up) scanned in 51.525 seconds
```

Nmap常见扫描类型及其解释

常见扫描类型	解释
-sT	TCP connect（）扫描。这是最基本的TCP扫描方式。这种扫描很容易被检测到，在目标主机的日志中会记录大批的连接请求以及错误信息。
-sS	TCP同步扫描。通过发出一个TCP同步包，然后等待回应。若对方返回SYN|ACK包就表示目标端口正在监听；若返回RST数据包，就表示目标端口没有监听程序；若收到一个SYN|ACK包，源主机就会马上发出一个RST数据包断开和目标主机的连接。
-sP	Ping扫描。若只是想知道此时网络上哪些主机正在运行。通过向指定的网络内的每个IP地址发送ICMP echo请求数据包，Nmap就可以完成这项任务，如果主机正在运行就会作出响应。
-sU	UDP扫描。通过该扫描方法可知某台主机提供哪些UDP服务。

Nmap常用通用选项及其解释

常见通用选项	结束
-O	用以激活对TCP/IP指纹特征的扫描，获得远程主机。
-sO	用以对远程主机所支持的IP协议进行扫描。
-sV	用以对主机服务的版本号进行扫描。
-p	用以选择要进行扫描的端口号的范围。

扫描技术

基本方法：**ping 扫描**

- （传统意义上）**ping**：向目标发ICMP ECHO（类型8）数据包，如返回 ICMP ECHO_REPLY数据包（类型0），说明目标系统真实存在
  - ✓ping
  - ✓nmap –sP：Linux + windows，GUI版本为Zenmap
- （现在的）**ping**：可利用 ICMP，TCP，UDP

```
root@kali:~# nmap -sP 58.218.185.156

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-15 09:01 CST
Nmap scan report for 58.218.185.156
Host is up (0.00081s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

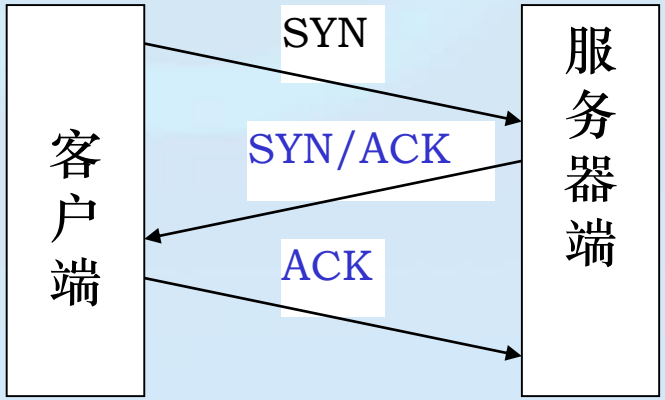
```
root@kali:~# nmap -sP www.cumt.edu.cn

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-15 08:58 CST
Nmap scan report for www.cumt.edu.cn (58.218.185.156)
Host is up (0.0020s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

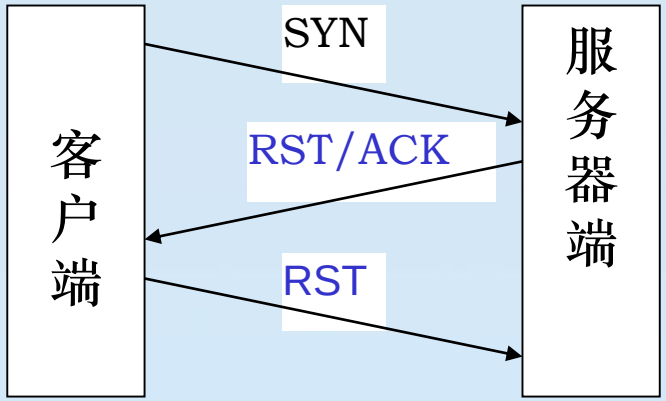
扫描技术

➢扫描类型：

1. TCP连接扫描（TCP Connect()扫描;nmap -sT）：连接目标端口并完成一次完整的三次握手过程；很容易被目标系统觉察



建立连接成功（目标端口开放）



未建立连接成功(目标端口关闭)

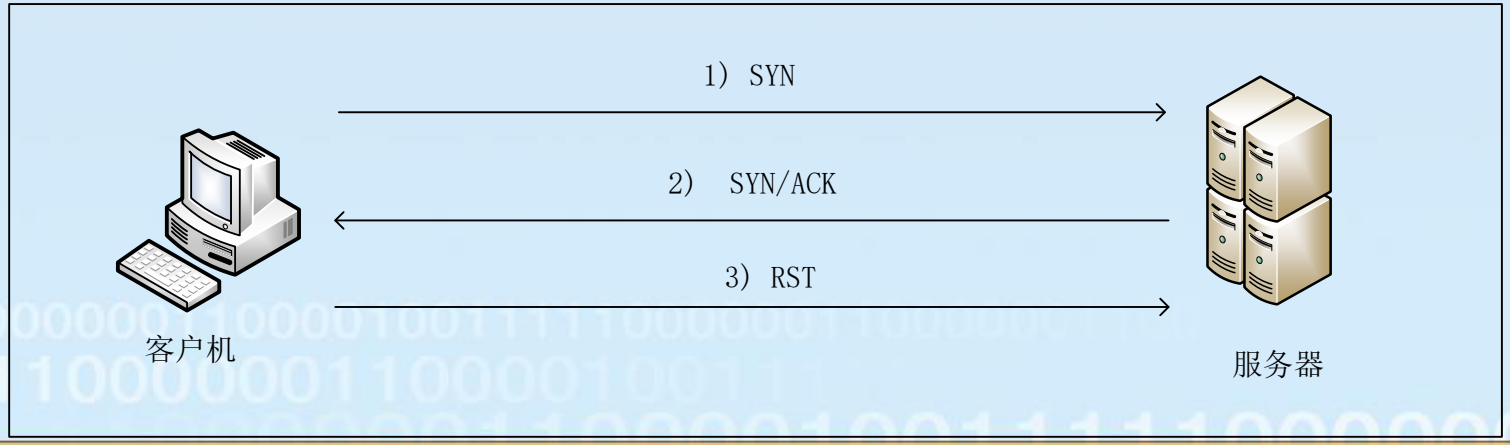
扫描技术

2. **TCP SYN扫描(半开扫描;nmap -sS)：向目标端口送SYN数据包**
   - 返回SYN/ACK数据包，可以断定该端口处于监听状态
   - 返回RST/ACK数据包，通常表明该端口不在监听状态

   然后，扫描者送出一个RST/ACK数据包（使通信双方永远不会建立一条完整连接）

   优点：更隐秘，目标系统一般不会将其记入日志

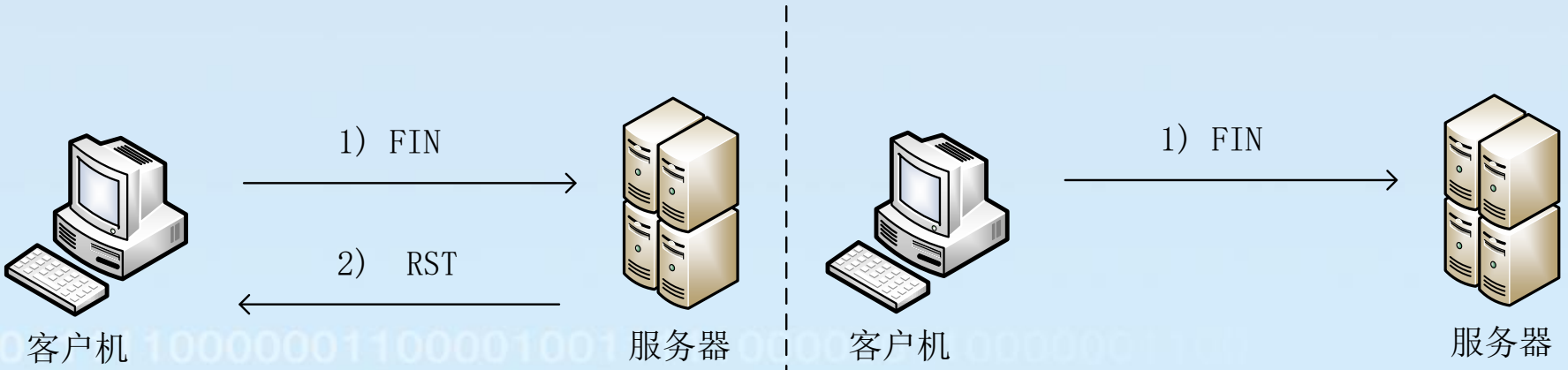
   缺点：半开连接过多时，会形成一种“拒绝服务”条件而引起对方的警觉



扫描技术

3. TCP FIN扫描(秘密扫描;nmap -sF)：向目标端口发送FIN数据包

- ✓ 如果目标端口关闭，目标系统应该返回一个RST数据包，否则丢弃该包。通常只对UNIX系统的TCP/IP栈有效（Window平台总是返回RST包）
- ✓ 由于不包含TCP三次握手协议的任何部分，所以无法被记录下来，从而比SYN扫描隐蔽
- ✓ FIN数据包能通过监测SYN包的包过滤器(秘密扫描)



(a)端口关闭的情况　　(b)端口开放的情况

扫描技术

秘密扫描的两个变体：

3.1 TCP Xmas扫描（圣诞树扫描;nmap -sX）：TCP包包头设置所有标志位

- 目标端口关闭，目标系统应该返回一个RST数据包

3.2 TCP Null扫描（空扫描;nmap -sN）：关掉所有的标志

- 目标端口关闭，目标系统应该返回一个RST数据包

✓ **Remark:** 使用这些组合的目的是通过FIN标记监测器的过滤

✓ **Remark:** 主要用于UNIX/Linux/BSD的TCP/IP的协议栈；不适用于Windows系统

扫描技术

4. TCP ACK扫描(nmap -sA)：测试防火墙的规则集。判断防火墙是简单的包过滤防火墙；还是高级的、具备数据包过滤功能的状态（stateful）防火墙
   - 不能用来确定端口是否开放或者关闭
5. TCP窗口扫描(nmap -sW)：测试特定目标系统（如AIX和FreeBSD系统）上的端口是否开放、被过滤——会导致目标系统返回不同的TCP窗口长度值

```
root@kali:~# nmap -sS mail.cumt.edu.cn

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-15 09:14 CST
Nmap scan report for mail.cumt.edu.cn (58.218.185.21)
Host is up (1.2s latency).
Not shown: 988 closed ports
PORT     STATE    SERVICE
25/tcp   open     smtp
80/tcp   open     http
110/tcp  open     pop3
111/tcp  open     rpcbind
143/tcp  open     imap
465/tcp  open     smtps
514/tcp  filtered shell
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
5989/tcp open     wbem-https
9900/tcp open     iua

Nmap done: 1 IP address (1 host up) scanned in 475.87 seconds
```

扫描技术

6. **TCP Maimon扫描(nmap -sM)：探测报文改为FIN/ACK外，其原理与TCP FIN扫描一样；无论端口是否开放，都应响应RST报文。Uriel注意到如果端口开放，许多基于BSD的系统只是丢弃该报文**

7. **UDP扫描(nmap -sU)：向目标端口发出UDP数据包**
   - 如果返回“ICMP port unreachable” 出错消息，表明端口关闭
   - 如果没有收到该消息，端口可能开放

   - remark：UDP不要求必须建立一条连接，所以扫描的准确性取决于与目标网络的使用情况和过滤机制有关的许多因素（**扫描结果不可靠**）

扫描技术

- **Q：目标站点阻断了ICMP数据包，怎么办？**

- **A：使用TCP，UDP进行ping扫描**
  - ✓ nmap –PT：对“-PT”选项指定的端口（通常是80端口）进行TCP ping扫描； 该选项向目标网络发出TCP ACK数据包并根据返回的RST数据包判断活跃主机

```
root@kali:~# nmap -sP -PT80 www.163.com
```

  - ✓ **problem：**为什么选用发出ACK数据包?
  - ✓ **answer：**绝大多数无状态（non-stateful）防火墙产品（如Cisco IOS系列）通常都会放行这种数据包

扫描技术

确定目标系统上哪些服务正在运行或监听

- **端口扫描：主动连接目标系统的TCP和UDP端口以确定哪些服务正在运行或处于LISTENING（监听）状态**

- **主要目的：**
  - ✓确定运行的TCP/UDP服务
  - ✓确定操作系统的具体类型
  - ✓确定提供服务的应用程序名称和版本

端口扫描的对策：

- 使用入侵检测系统

- 设置防火墙过滤规则，阻止对端口的扫描：例如可以设置检测SYN扫描而忽略FIN扫描

- 禁止所有不必要的服务，把自己的暴露程度降到最低：Unix或linux中，在/etc/inetd.conf中注释掉不必要的服务，并在系统启动脚本中禁止其他不必要的服务；Windows中通过Services禁止敏感服务，如IIS

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	Pof，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
网络服务被动辩视技术	被动监测网络通信以识别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**
  - ✓ 为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

栈指纹识别技术

- 定义：利用TCP/IP协议栈实现上的特点来辨识一个操作系统
- 原理：寻找不同操作系统之间在处理网络数据包上的差异，并且把足够多的差异组合起来，以便精确地识别出一个系统的OS版本
- 技术导向
  - ✓ 可辨识的OS的种类，包括哪些操作系统
  - ✓ 结论的精确度，细微的版本差异是否能识别
- 一些工具
  - ✓ Checkos, by Shok
  - ✓ Queso, by Savage
  - ✓ Nmap, by Fyodor
- 配置能力
  - ✓ 扩展性，新的OS，版本不断推出
  - ✓ 定义一种配置语言或者格式

主动式指纹识别技术

- **原理：**主要靠向对方主机发送一些特定的报文，并检查对方主机的回应。不同操作系统上往往会对这些特定的报文作出不同的反应，据此可以比消极地分析对方发送的数据更加精确地判断对方的操作系统。
- **常用的手段**
  - ✓ 给一个开放的端口发送FIN包，有些操作系统有回应，有的没有回应
  - ✓ 对于非正常数据包的反应
    - 发送一个包含未定义TCP标记的数据包
  - ✓ 根据TCP连接的序列号风格
    - 寻找初始序列号之间的规律
  - ✓ ACK值
    - 有些系统会发送回所确认的TCP分组的序列号，有些会发回序列号加1
  - ✓ TCP初始化窗口
    - 有些操作系统会使用一些固定的窗口大小
  - ✓ DF位(Don't Fragment bit)
    - 某些操作系统会设置IP头的DF位来改善性能

被动式指纹识别技术

- 是一种类似于嗅探的“安静”的指纹识别。它不会向网络中发送任何报文，整个过程仅仅是监听目标主机与其它主机的通信。
- 在共享式网络中可以方便地直接进行此类攻击。但在交换网络中，则必须先通过攻击交换机或对目标主机进行ARP欺骗，以使目标主机的流量经过本机。
- 不是向目标系统发送分组，而是被动监测网络通信，以确定所用的操作系统
  - ✓ 如根据TCP/IP会话中的几个属性：
    - TTL
    - 窗口大小
    - DF
    - TOS
  - ✓ Siphon工具，http://siphon.datanerds.net/

扫描技术—操作系统探测

- **可用的探查技术：**
  - ✓ **FIN探查**：向某个打开端口发出FIN数据包。根据RFC 793的规定，目标系统应该不做任何响应。但许多实现如Windows会返回FIN/ACK数据包
  - ✓ **无效标志探查**：在SYN数据包的TCP报头置位一个未定义的TCP标志。某些操作系统（如Linux）会在响应数据包里置位这个标志
  - ✓ **ISN（Initial Sequence Number，初始序列号）采样：** TCP协议在响应一个连接请求时，返回的ISN呈现不同的模式
  - ✓ **DF标志位监控：**某些操作系统会置位DF位（Don't Fragment）以改善性能

扫描技术—操作系统探测

- **可用的探查技术（续）：**
  - ✓ **TCP初始数据窗长度**：目标系统返回数据包的初始窗口大小不同
  - ✓ **ACK值**：不同的IP协议栈在往ACK字段里填写序列号时会采用不同的做法，有的原封不动地送回，有的则会先加1、再送回来
  - ✓ **ICMP出错消息抑制**（有些OS会对送出ICMP出错消息的频率做出限制）/**ICMP消息内容**（不同OS在ICMP返回消息里给出的文字内容不一样）/**ICMP出错消息——请求/响应是否匹配**（某些实现在返回ICMP出错消息时会改变请求数据包的IP报头）
  - ✓ **数据包拆分处理：**协议栈在处理数据包分片时采取不同的做法。在重新组合数据包时，协议栈会用后收到的新数据覆写先收到的老数据（或者相反）

扫描技术—操作系统探测

```
root@kali:~# ping -c 4 192.168.40.128
PING 192.168.40.128 (192.168.40.128) 56(84) bytes of data.
64 bytes from 192.168.40.128: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 192.168.40.128: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 192.168.40.128: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 192.168.40.128: icmp_seq=4 ttl=64 time=0.048 ms

--- 192.168.40.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.048/0.055/0.064/0.006 ms
root@kali:~# ping -c 4 192.168.40.130
PING 192.168.40.130 (192.168.40.130) 56(84) bytes of data.
64 bytes from 192.168.40.130: icmp_seq=1 ttl=128 time=0.533 ms
64 bytes from 192.168.40.130: icmp_seq=2 ttl=128 time=0.645 ms
64 bytes from 192.168.40.130: icmp_seq=3 ttl=128 time=0.263 ms
64 bytes from 192.168.40.130: icmp_seq=4 ttl=128 time=0.149 ms

--- 192.168.40.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.263/0.448/0.645/0.149 ms
```

ubuntu linux、Win 7

windows XP

扫描技术—操作系统探测

- **主动协议栈指纹分析技术：**向目标系统发送数据包去探查网络协议栈的独有特点，推测操作系统
  - nmap –O：同时使用以上技术（“数据包拆分处理”和“ICMP出错消息队列”除外）进行探查

```
root@kali:~# nmap -O 192.168.40.130

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-15 09:24 CST
Nmap scan report for 192.168.40.130
Host is up (0.00057s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
143/tcp  open  imap
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
465/tcp  open  smtps
993/tcp  open  imaps
995/tcp  open  pop3s
1025/tcp open  NFS-or-IIS
6000/tcp open  X11
MAC Address: 00:0C:29:2A:10:F3 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
```

扫描技术—操作系统探测

- **被动协议栈指纹分析技术：**通过被动地监控网络通信推测目标的操作系统
  - 成功取决于攻击者必须位于网络的通信枢纽，以及必须有一个可用来捕获数据包的端口
  - **(部分)被动式特征**:TTL/窗口大小/DF位
    - ✓siphon的指纹数据库文件osprints.conf

```
# Send new fingerprints to siphon@subterrain.net

# Window:TTL:DF:Operating System
# DF = 1 for ON, 0 for OFF.

7D78:64:1:Linux 2.1.122 - 2.2.14
77C4:64:1:Linux 2.1.122 - 2.2.14
7BF0:64:1:Linux 2.1.122 - 2.2.14
7BC0:64:1:Linux 2.1.122 - 2.2.14
832C:64:1:Linux 2.0.34 - 2.0.38
7FE0:64:0:Linux 2.0.34 - 2.0.38
0B68:64:1:Linux 2.0.32 - 2.0.34

4470:64:0:FreeBSD 2.2.1 - 4.0
4470:64:1:FreeBSD 2.2.1 - 4.0
43E0:64:1:FreeBSD 2.2.1 - 4.0
4074:64:0:OpenBSD 2.x
43E0:64:0:OpenBSD 2.x
4000:64:0:NetBSD 1.3 - 1.33 / AIX 4.3.X
```

被动式指纹识别技术

例子：

telnet 192.168.102.245（发起方为192.168.102.155 ）

利用snort监听到的数据包：

192.168.102.245:23-> 192.168.102.155:2300

TCP TTL:255 TOS:0x0 ID:58955 DF

S*A* Seq:0xD3B709A4 Ack:0xBE09B2B7 Win:0x2798

TCP Options => NOP NOP TS:9688775 9682347 NOP WS:0 MSS:1460

和osprints.conf比较， 可猜测192.168.102.245的操作系统为

Solaris 2.6-2. 7

漏洞扫描

- **漏洞**
  - ✓ Security Vulnerability，安全脆弱性
  - ✓ 一般任务，漏洞是指硬件、软件或策略上存在的安全缺陷，从而使得攻击者能够在未授权得情况下访问、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.mocrosoft.com/china/technet/security/current.mspx)
  - ✓ SecurityFocus BID (http://www.securitfocus.com/bid)
  - ✓ National Vulnerability Database:NVD (http://nvd.nist.gov/)

漏洞扫描

迅睿CMS存在命令执行漏洞（CNVD-2021-62062）

报送者:Jiang

CNVD-ID	CNVD-2021-62062
公开日期	2031-09-28
危害级别	高 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
影响产品	四川迅睿云软件开发有限公司 迅睿CMS 4.5.1
漏洞描述	迅睿CMS是一款基于CodeIgniter4开发的内容管理框架。 迅睿CMS存在命令执行漏洞，攻击者可利用该漏洞获取服务器控制权。
漏洞类型	通用型漏洞
URL	
参考链接	
临时解决方案	下载网站最新版的代码
正式解决方案	厂商尚未提供漏洞修复方案 ms.com/
厂商补丁	(无补丁信息)
验证信息	迅睿CMS存在命令执行漏洞
报送时间	2021-08-06
收录时间	2021-08-16
更新时间	2022-03-25
漏洞附件	关于迅睿CMS存在命令执行漏洞的情况通报.docx
中间件	其他
类型	其他
利用工具	浏览器

攻击途径：远程网络　**攻击复杂度**：低
认证：不需要认证　**机密性**：完全地
完整性：完全地　**可用性**：完全地

漏洞评分 ： 10.0

在发布漏洞公告信息之前，CNVD都力争保证每条公告的准确性和可靠性。然而，采纳和实施公告中的建议则完全由用户自己决定，其可能引起的问题和结果也完全由用户承担。是否采纳我们的建议取决于您个人或您企业的决策，您应考虑其内容是否符合您个人或您企业的安全策略和流程。

漏洞扫描存在的问题：

- 漏洞库的完整性问题
- 检测的准确性
- 漏洞库的及时更新问题
- 系统的安全评估问题

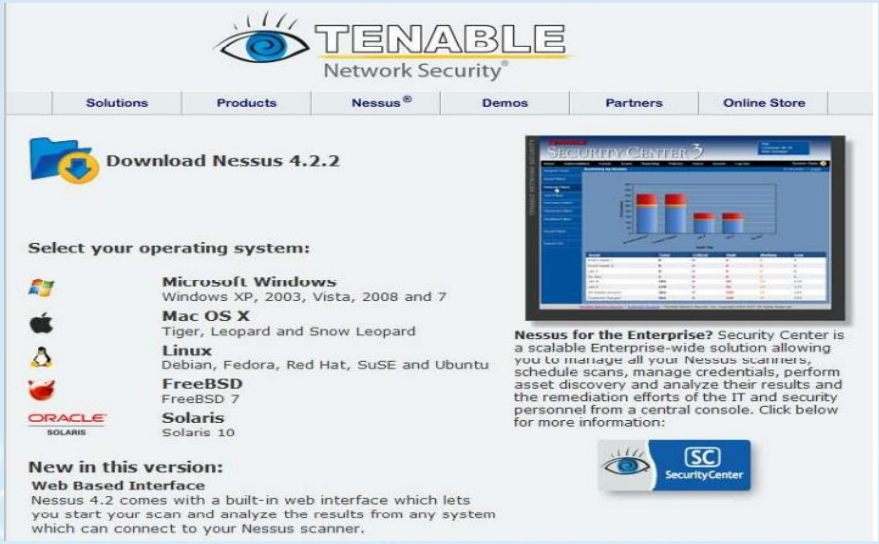
漏洞扫描

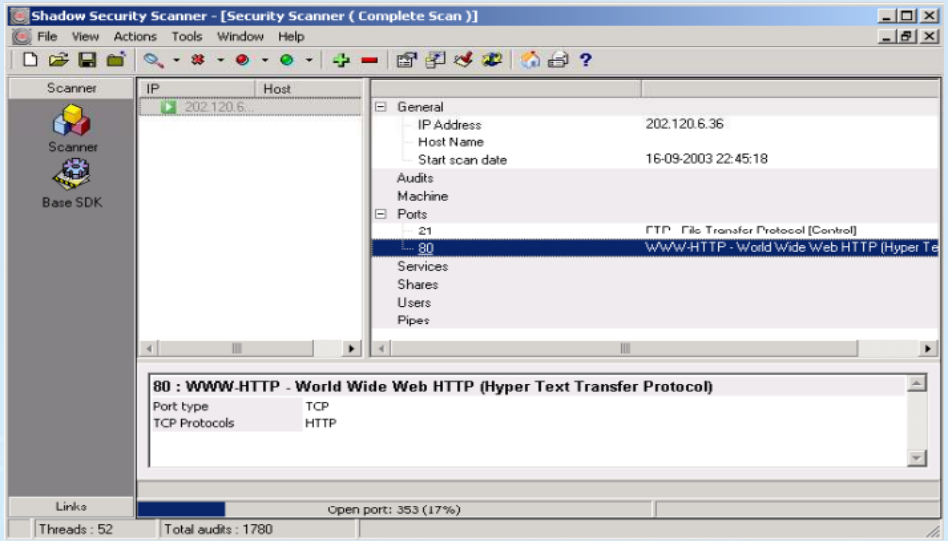
- 安全漏洞的探测工具——Nessus

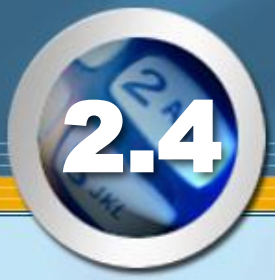
下载地址：http://www.nessus.org/download/

- 安全漏洞的探测工具——SSS

SSS(Shadow Security Scanner)是俄罗斯的一个黑客团体开发的在Windows系统中运行的远程漏洞探测工具。







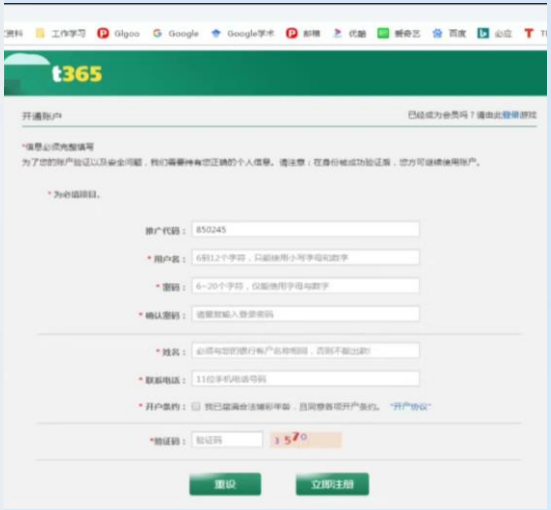
信息收集实验

实验任务：熟练使用 Nmap进行网络扫描实验

实验原理：通过主机扫描确定网络中的目标活动主机后，使用端口扫描技术对目标主机进行端口扫描可以得到目标主机开放的服务程序和运行的系统版本等信息，从而为下一步的系统或漏洞扫描做准备。

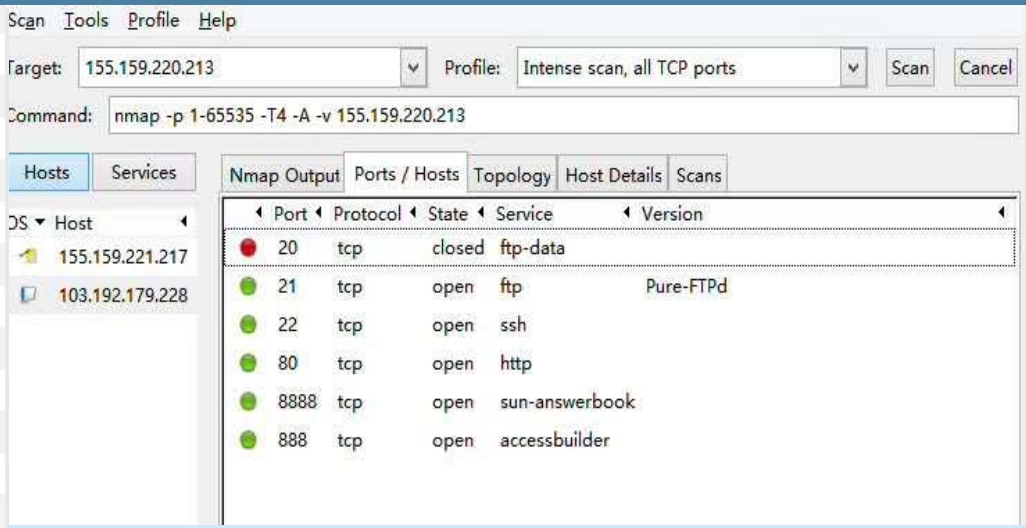
- 场景1:警方得到内线消息，抓获一经营违法网站的黑客，并从其电脑取出一远程连接的可疑ip地址112.121.185.83，然而该服务器上似乎并没有运行非法网站。警方想挖出其犯罪证据，同时找出该罪犯经营的所有非法网站及服务器并封杀。领导将此重任委托给了你，你能解决这个问题吗？

域名及相关信息吗？



7	175f41hm.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns17.hichina.com dns18.hichina.com	2020-03-08 2021-03-08
8	57145mk4.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns23.hichina.com dns24.hichina.com	2020-03-08 2021-03-08
9	92859qw1.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns29.hichina.com dns30.hichina.com	2020-03-08 2021-03-08
10	4374f54.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns11.hichina.com dns12.hichina.com	2020-03-08 2021-03-08
11	613ru47.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns25.hichina.com dns26.hichina.com	2020-03-08 2021-03-08
12	tmyggcw.cn	无锡市振森设备安装有限公司	--	阿里巴巴云计算（北京）有限公司	dns29.hichina.com dns30.hichina.com	2020-03-07 2021-03-07
13	ottrqdv.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns15.hichina.com dns16.hichina.com	2020-03-01 2021-03-01
14	gnezzod.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns11.hichina.com dns12.hichina.com	2020-03-01 2021-03-01
15	aulqtnu.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns25.hichina.com dns26.hichina.com	2020-03-01 2021-03-01
16	kkvgklx.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns19.hichina.com dns20.hichina.com	2020-03-01 2021-03-01
17	wtyaudw.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns15.hichina.com dns16.hichina.com	2020-02-26 2021-02-26
18	atasajj.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns13.hichina.com dns14.hichina.com	2020-02-26 2021-02-26
19	euuwwtf.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns4.hichina.com dns3.hichina.com	2020-02-26 2021-02-26
20	bbnileg.cn	尹红爱	--	阿里巴巴云计算（北京）有限公司	dns17.hichina.com dns18.hichina.com	2020-02-22 2021-02-22

导出数据 找到 12802 条记录 1 2 3 4 5 6 7 > >> 共641页，到第 页 确定



Scan Tools Profile Help

Target: 155.159.220.213 Profile: Intense scan, all TCP ports Scan Cancel

Command: nmap -p 1-65535 -T4 -A -v 155.159.220.213

Hosts Services

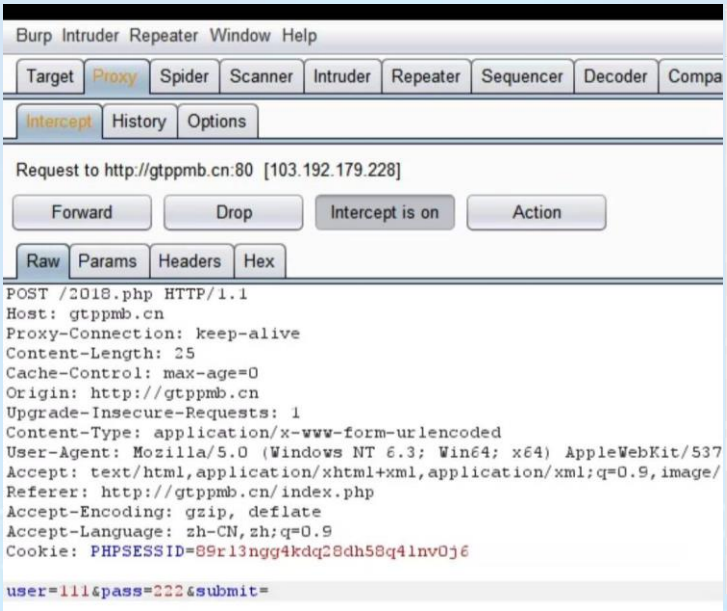
OS Host

155.159.221.217

103.192.179.228

Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
20	tcp	closed	ftp-data	
21	tcp	open	ftp	Pure-FTPd
22	tcp	open	ssh	
80	tcp	open	http	
8888	tcp	open	sun-answerbook	
888	tcp	open	accessbuilder	



Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compa

Intercept History Options

Request to http://gtppmb.cn:80 [103.192.179.228]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /2018.php HTTP/1.1
Host: gtppmb.cn
Proxy-Connection: keep-alive
Content-Length: 25
Cache-Control: max-age=0
Origin: http://gtppmb.cn
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
Referer: http://gtppmb.cn/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=89rl3ngg4kdq28dh58q4lnvOj6

user=111&pass=222&submit=
```

whois查询 最新注册 邮箱反查 注册人反查 电话反查 域名批量反查

gtppmb.cn

域名 gtppmb.cn 的信息 以下信息更新时间：2020-05-28 17:41:33 立即更新

域名	gtppmb.cn [whois 反查] 其他常用域名后缀查询： cn com cc net org
注册商	阿里云计算有限公司（万网）
联系人	常州雅贝木业有限公司 [whois反查]
联系邮箱	**71440@qq.com [whois反查]
创建时间	2019年06月30日
过期时间	2020年06月30日
DNS	dns15.hichina.com dns16.hichina.com
状态	域名普通状态(ok)

iP或域名查询

103.192.179.228 X 查询

中国 香港

103.192.179.228上的网站

绑定过的域名如下：

wgtbkk.cn	2020-05-26-----2020-05-26
z2zjie.cn	2020-05-24-----2020-05-24
z2zyang.cn	2020-05-24-----2020-05-24
z2qyuan.cn	2020-05-23-----2020-05-23
ad-chezhuwuyou.com	2019-09-09-----2019-09-13

在103.192.179.0/24查找网站