信息安全导论

第七章 网络安全

黄 玮

温故

- 安全操作系统
- 主流操作系统的安全策略与安全机制

知新

- 网络安全概述
- 网络与系统渗透
- 网络与系统防御

本章内容提要

- **网络安全概述**
- 网络与系统渗透
- 网络与系统防御

专业术语与概念定义（1/3）

- 交换机
  —Switch
- 客户端
  —Client
- 服务器
  —Server
- 骨干网 / 广域网 / 局域网
- 虚拟主机 / VPS / 主机托管

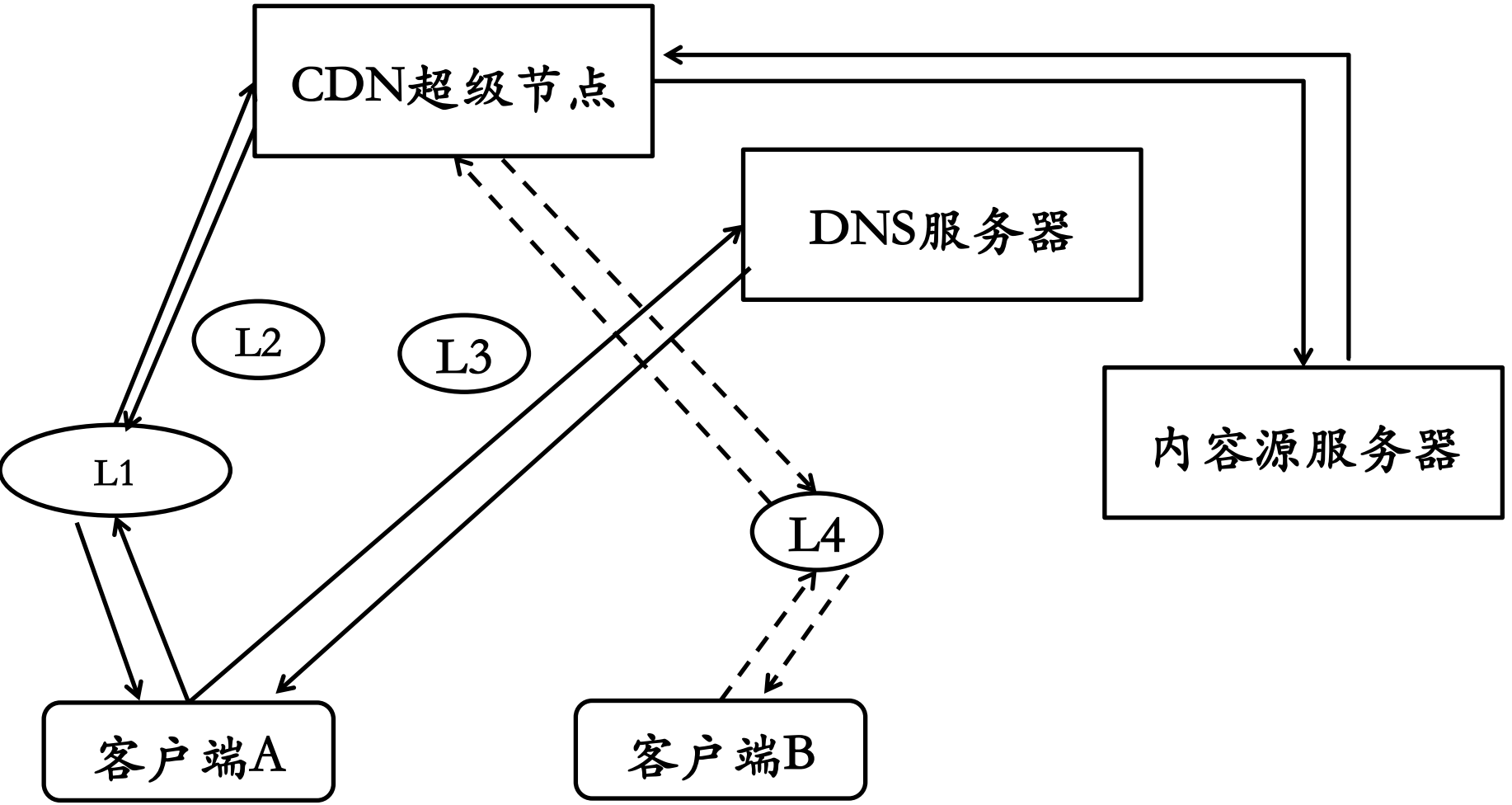
专业术语与概念定义（2/3）

- 域名解析服务器
  - —DNS: Domain Name System
  - —域名解析：将域名翻译、转换成IP地址
- Web服务器
  - —Web Server：Static Page Serve
- 应用程序服务器
  - —App Server：Dynamic Pages Serve
- 数据库服务器
  - —Database Server

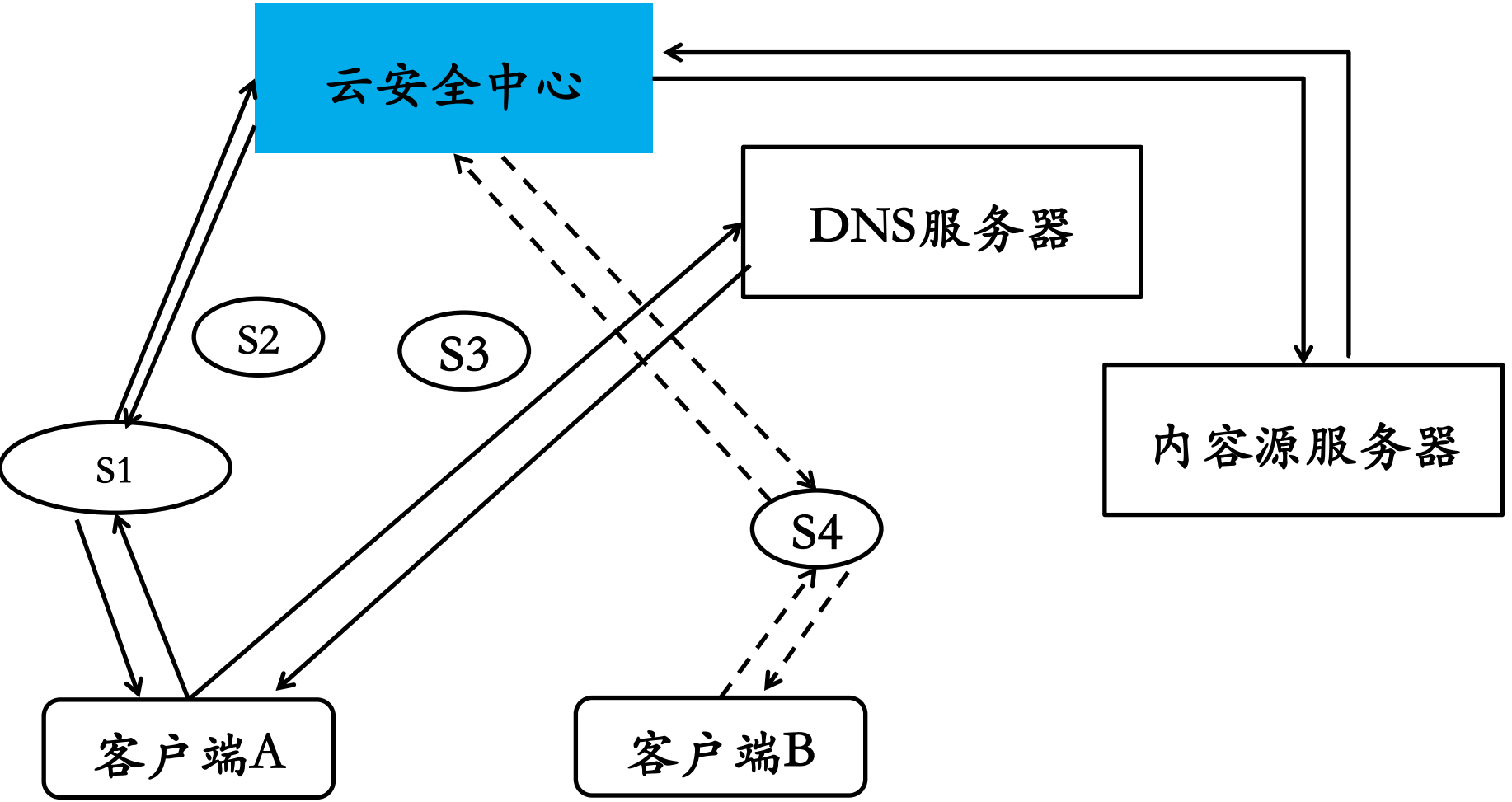
专业术语与概念定义（3/3）

- 网络渗透/系统渗透
  —Network Penetration / System Penetration
- Nmap
  —网络扫描的瑞士军刀
- 内容分发网络
  —CDN: Content Delivery Network

内容分发网络



云防火墙



云安全?

- 基于CDN的云安全
  - —保护第三方Web站点
- 云计算安全
  - —IDC安全
  - —VPS安全
  - —Web安全

新概念不断，
但网络安全的基本原理并没有改变

本章内容提要

- 网络安全概述
- 网络与系统渗透
- 网络与系统防御

网络与系统渗透的入口点选择——技术方向

- nmap官方对互联网上端口开放频率的统计
  - —sort -rk 3 /usr/share/nmap/nmap-services
    - http 80/tcp 0.484143 # World Wide Web HTTP
    - https 443/tcp 0.208669 # secure http (SSL)
- Web应用是最常见的网络渗透入口点
- Web软件是最普遍的云服务实现载体
  - —云存储：Dropbox、DBank等
  - —即时通信：腾讯Web QQ
  - —微博：新浪微博、腾讯微博
  - —视频：优酷、奇艺、腾讯视频

Web应用系统服务模型

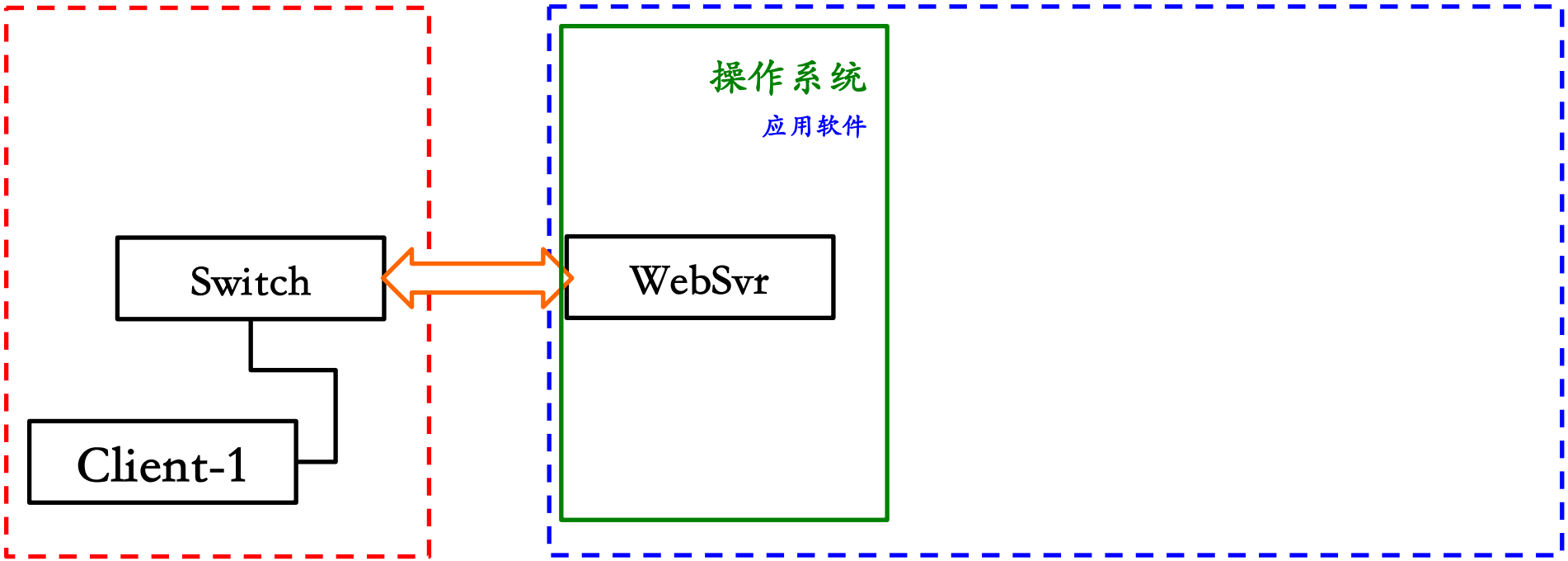
网络攻击的基本原理

- 网络攻击的过程可以看作是一个恶意数据输入的过程
  - ——关键是堵住漏洞的入口点
    - 核心是软件或硬件存在安全漏洞
    - 病从口入原理

Web应用系统网络拓扑（1/6）

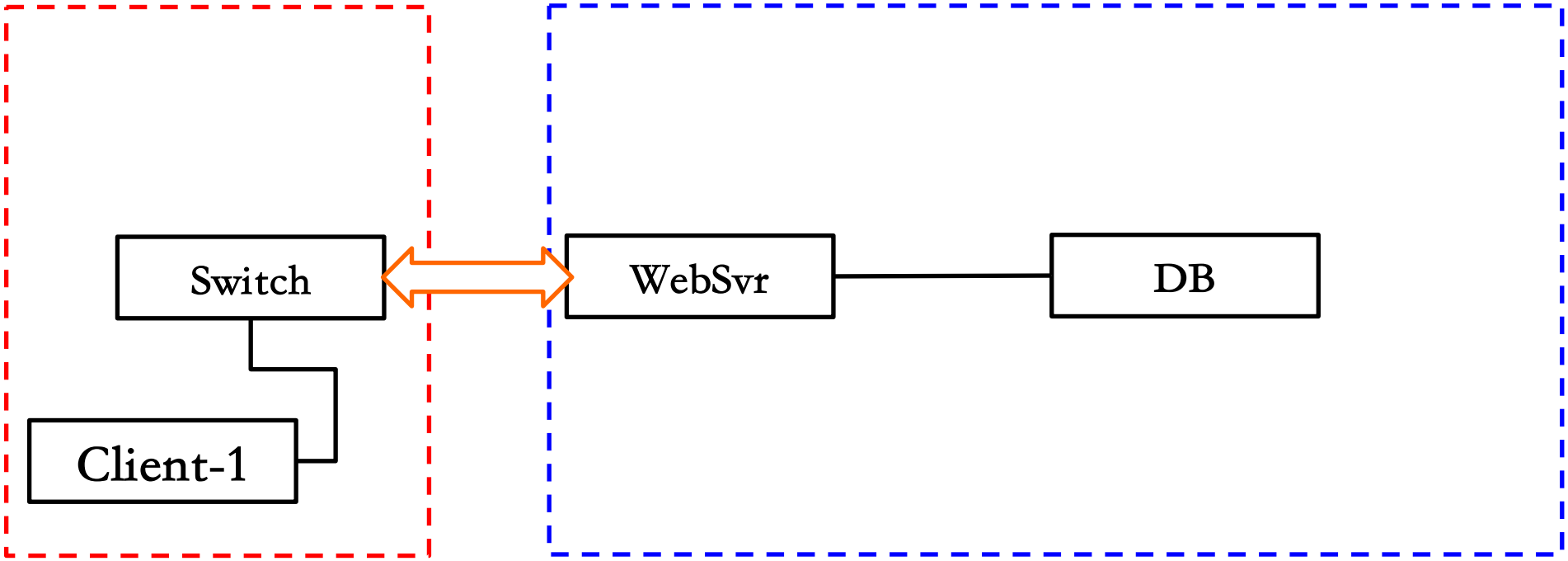
- 最基本的静态网页服务

  ——会被攻击吗？

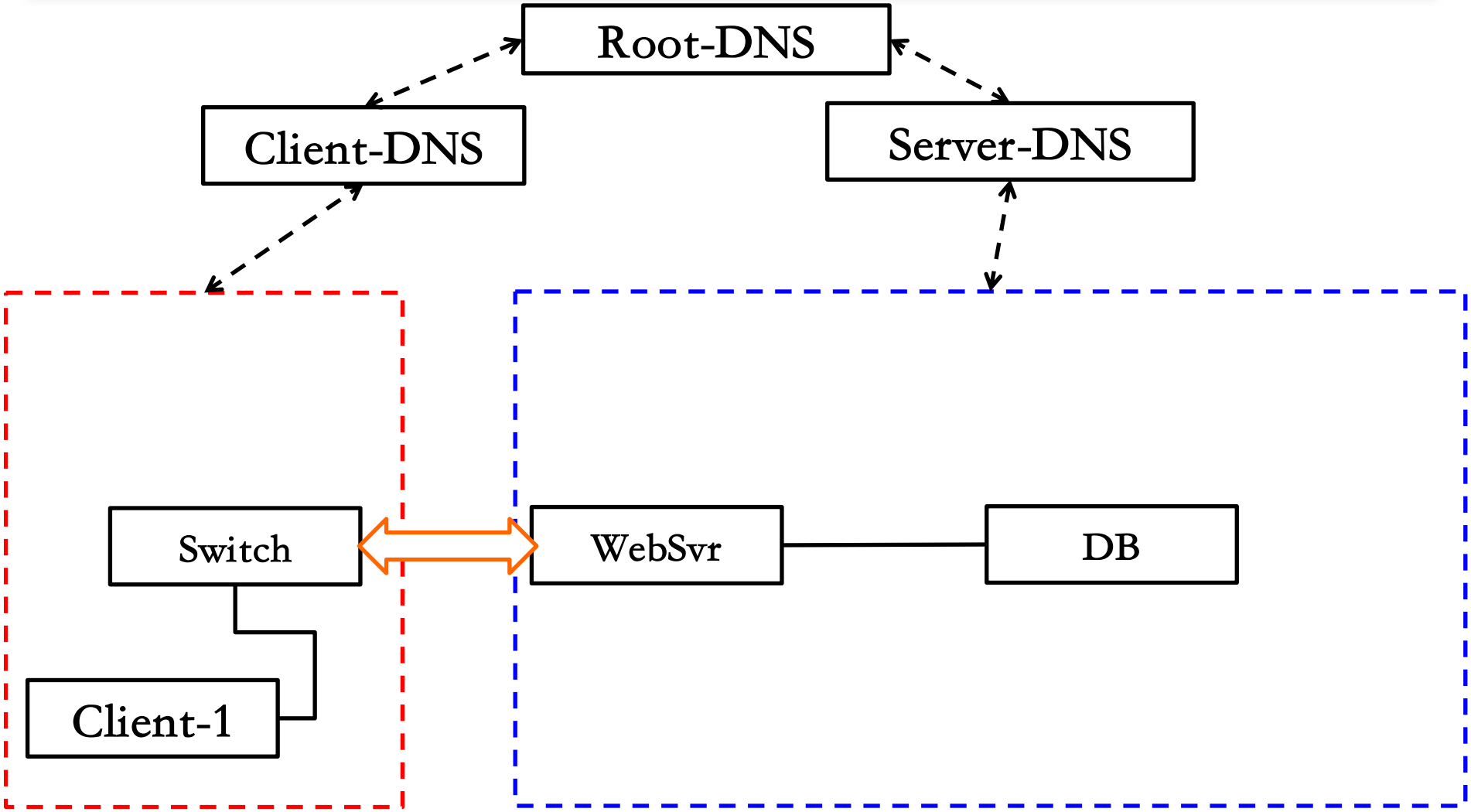


Web应用系统网络拓扑（2/6）

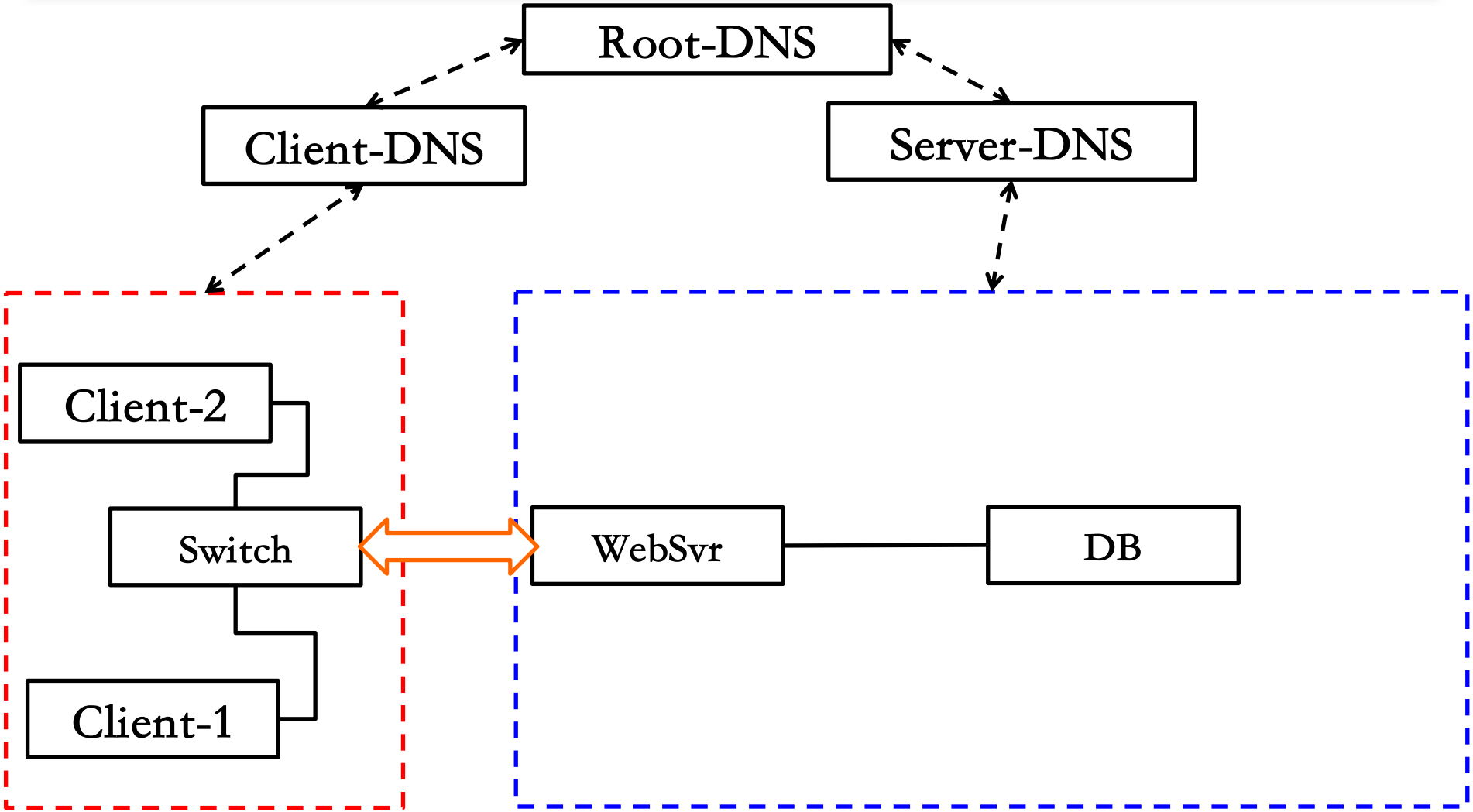
- 最基本的动态网页服务



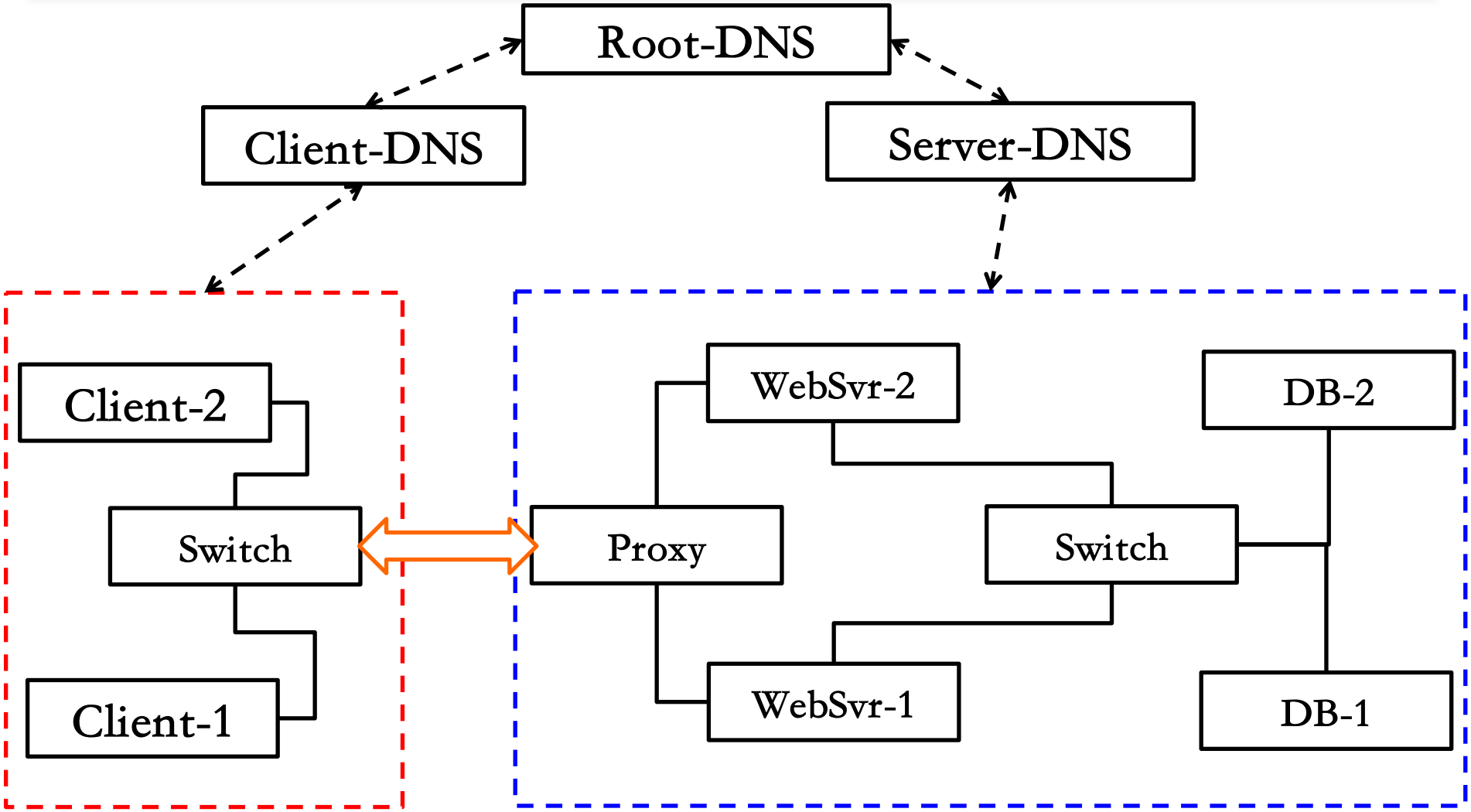
Web应用系统网络拓扑（3/6）



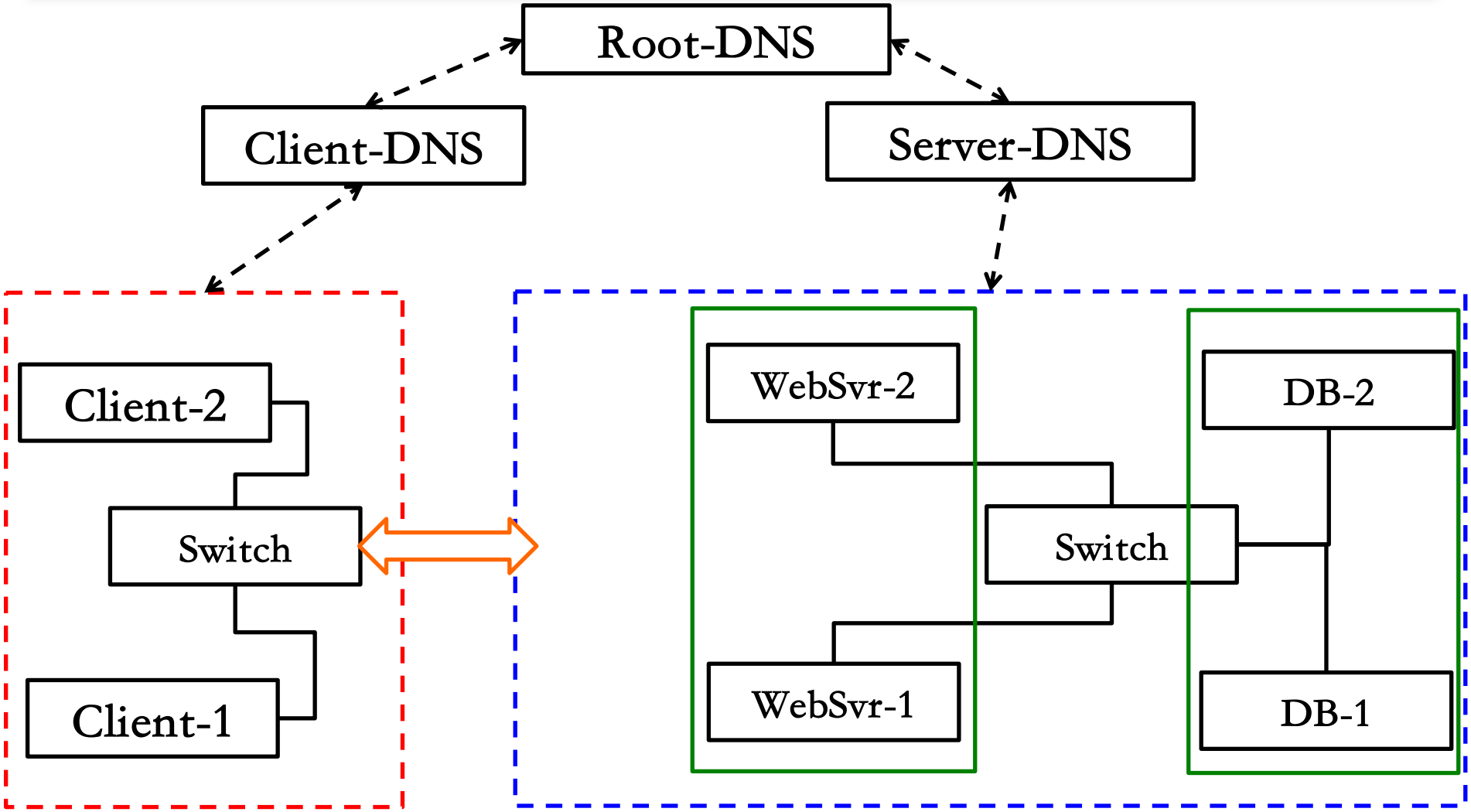
Web应用系统网络拓扑（4/6）



Web应用系统网络拓扑（5/6）



Web应用系统网络拓扑（6/6）--共享式虚拟主机



客户端一侧的可能攻击方式

- ARP攻击
- DNS投毒
  - 本地主机的hosts文件投毒
  - 局域网DNS投毒
  - 局域网路由器DNS篡改
  - ARP攻击篡改
- 内网攻击

服务器一侧可能的攻击方式

- 旁站攻击
  - 单个主机上同时运行
    - 多个Web Server实例
    - 多个DB实例
- ARP攻击
- DNS投毒（同客户端一侧）
- Web应用漏洞攻击

针对基础服务的攻击方式

- DNS服务器攻击
  - 篡改DNS配置
  - 停止DNS解析服务
- 攻击DNS后台管理控制台
  - 篡改DNS配置
- 攻击CDN服务器
  - 篡改缓存

渗透测试与网络入侵的一般区别与联系

渗透测试

- 目的
  - —发现漏洞，提出漏洞修补建议
- 手段
  - —在保证被测试系统的业务连续性和数据完整性的前提条件下，尝试各种漏洞利用手段
- 结果
  - —渗透测试报告
  - —所有已发现漏洞得到修补

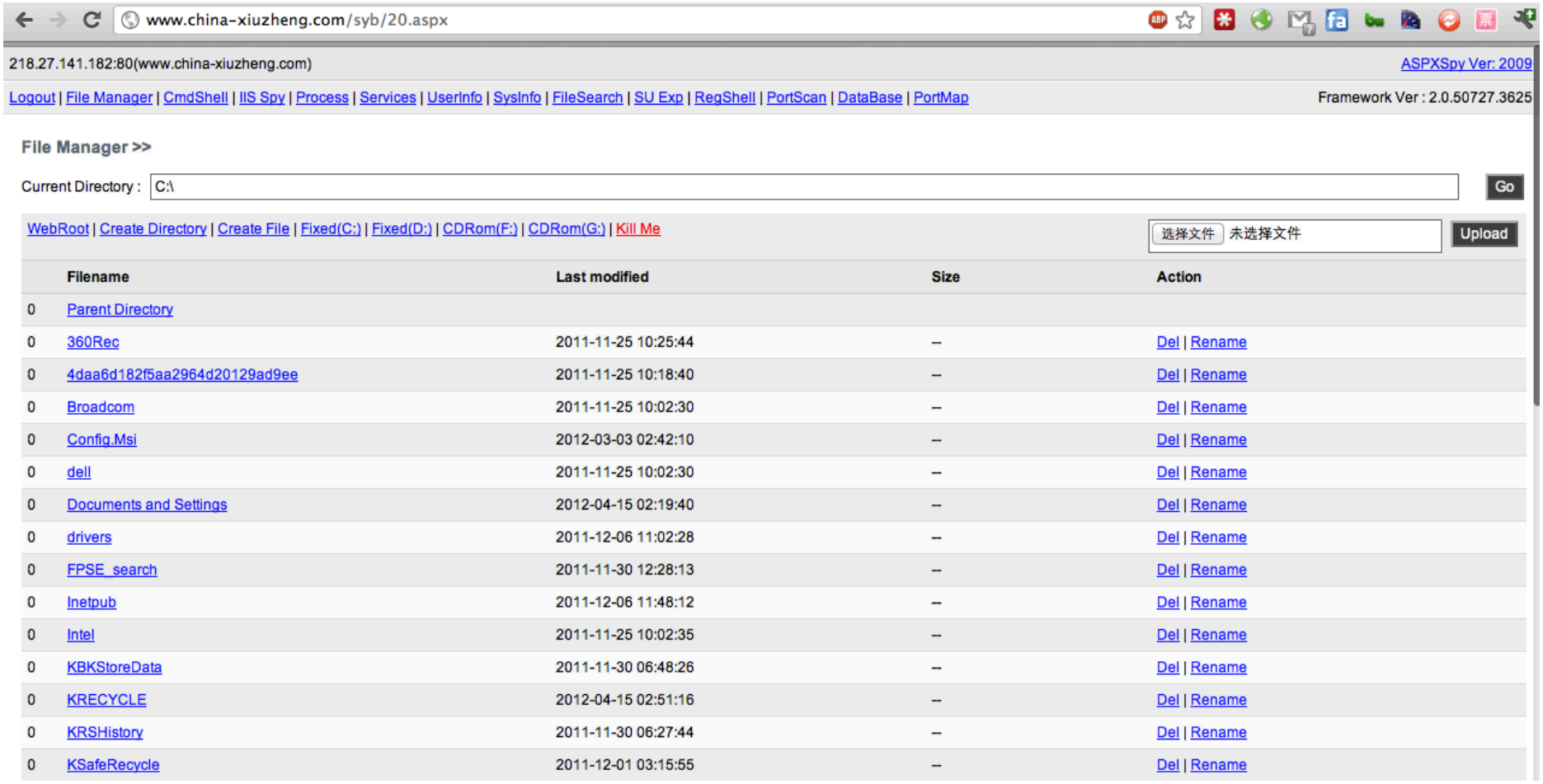
网络入侵

- 目的
  - —获取系统控制权
  - —获取敏感信息
- 手段
  - —无限制的漏洞利用手段
- 结果
  - —系统被远程控制
  - —数据被非法访问和篡改
  - —业务连续性和服务质量受到影响

渗透测试与网络入侵的方法论区别与联系

渗透测试	网络入侵
• 取得被测试目标的法律授权	
• 信息收集	• 信息收集
• 目标踩点	• 目标踩点
• 网络扫描	• 网络扫描
• 漏洞发现 —漏洞扫描（识别已知漏洞） —漏洞挖掘（发现未知漏洞）	• 漏洞发现 —漏洞扫描（识别已知漏洞） —漏洞挖掘（发现未知漏洞）
• 漏洞利用 —提升权限	• 漏洞利用 —提升权限 —后门植入
• 提供测试报告	• 擦除痕迹

真实网络入侵案例——Web应用程序漏洞



	Filename	Last modified	Size	Action
0	Parent Directory			
0	360Rec	2011-11-25 10:25:44	--	Del | Rename
0	4daa6d182f5aa2964d20129ad9ee	2011-11-25 10:18:40	--	Del | Rename
0	Broadcom	2011-11-25 10:02:30	--	Del | Rename
0	Config.Msi	2012-03-03 02:42:10	--	Del | Rename
0	dell	2011-11-25 10:02:30	--	Del | Rename
0	Documents and Settings	2012-04-15 02:19:40	--	Del | Rename
0	drivers	2011-12-06 11:02:28	--	Del | Rename
0	FPSE_search	2011-11-30 12:28:13	--	Del | Rename
0	Inetpub	2011-12-06 11:48:12	--	Del | Rename
0	Intel	2011-11-25 10:02:35	--	Del | Rename
0	KBKStoreData	2011-11-30 06:48:26	--	Del | Rename
0	KRECYCLE	2012-04-15 02:51:16	--	Del | Rename
0	KRSHistory	2011-11-30 06:27:44	--	Del | Rename
0	KSafeRecycle	2011-12-01 03:15:55	--	Del | Rename

真实网络入侵案例——操作系统漏洞

真实网络入侵案例——弱口令

小结：用分层的方法来看Web威胁模型

- 人
- 配置管理缺陷
- XSS/CSRF/URL强制访问
- HTTP / DB 缓存投毒
- 后端(数据库/Web Service/ SOAP)注入
- 编程语言/ 编程框架 缺陷
- HTTP / APP/ DB / 缓存 服务器
- DNS / LDAP 服务器
- 操作系统
- 路由器/ 交换机
- 硬件(环境)

- 人
- 应用系统/服务
- 操作系统
- 网络基础设施
- IT物理环境

本章内容提要

- 网络安全概述
- 网络与系统渗透
- **网络与系统防御**

正确的安全观

- Built-in Security

  —内置安全

- Security by Default

  —默认安全

- Security in Depth

  —纵深防御

- Proactive Security

  —主动安全

- 能通过安全软件工程解决的问题，绝不依赖外围安全产品
  - —微软的安全开发生命周期
    - 安全思想、方法、技术融入到软件工程的每一个环节

Security by Default

- 默认配置
  - —用户名
  - —口令
  - —后台管理地址
- 默认最小化
  - —开启的功能数量
  - —开放的服务种类
  - —授权

Security in Depth

- 即使实施了安全软件工程，也要
  - —实时监控
  - —异构化应用、服务、系统和网络
  - —容灾备份机制

Proactive Security

- 定期实施
  - —风险评估
  - —渗透测试

安全防御与加固的常见手段（1/4）

- 安全需求分析
  - —识别资产、评估价值
  - —明确安全建设预计投入成本
  - —有的放矢，抓重点，加强安全短板
    - 等级安全保护原理
  - —建立持续安全机制
    - 不能期望一劳永逸

安全防御与加固的常见手段（2/4）

- 购买安全设备
  - —防火墙
  - —IDS/IPS
    - 入侵检测系统/入侵保护系统
  - —蜜罐
  - —蜜网
  - —UTM
    - 统一威胁管理

安全防御与加固的常见手段（3/4）

- 安全配置
  - —操作系统安全配置
  - —应用服务安全配置
    - – Web服务器安全配置
    - – SSH服务器安全配置
    - – DNS安全配置
    - – 版本控制器安全配置
    - – VPN服务器安全配置
  - —杜绝弱口令
    - – 弱口令扫描

安全防御与加固的常见手段（4/4）

- 渗透测试与风险评估
  - —模拟黑客攻击行为
    - 从攻击者角度重新审视网络与系统安全
  - —人员安全培训教育与安全测试
    - 专人负责制
- 建立安全监控与安全响应机制

课后思考题

- 用自己的话去阐述“网络与系统安全是一个持续对抗过程”。