# 典型案例内容

黛蛇：蠕虫

Morris:蠕虫

温柔、大小姐：木马；

红色代码、尼姆达和SQL Slammer：远程渗透攻击IIS / MS SQL

已知漏洞渗透代码来源：Metasploit、Exploit-db、Packetstorm、SecurityFoucs

# 概念

三个查点分类

## 网络踩点

1.有计划有步骤的信息情报搜集 2.了解到目标的网络环境和信息安全状况 3.得到攻击目标剖析图 4.通过对剖析图细致分析，找到薄弱环节，提供指引

## 网络扫描

探测网络，找出更多的连接目标（主机，端口，系统，漏洞）获取类型弱点等，为攻击选择目标，提供通道支持

## 漏洞产因：

1.系统设计缺陷（internet、TCP/IP协议栈 三次握手）2.操作系统内核代码量巨大 3.软件实现的缺陷

## 网络查点和扫描踩点的区别

1.入侵程度：踩点在外围收集信息，查点主动连接查询（会被IDS与日志记录）

2.针对性、目的性：踩点较大范围，查点有着明确目标

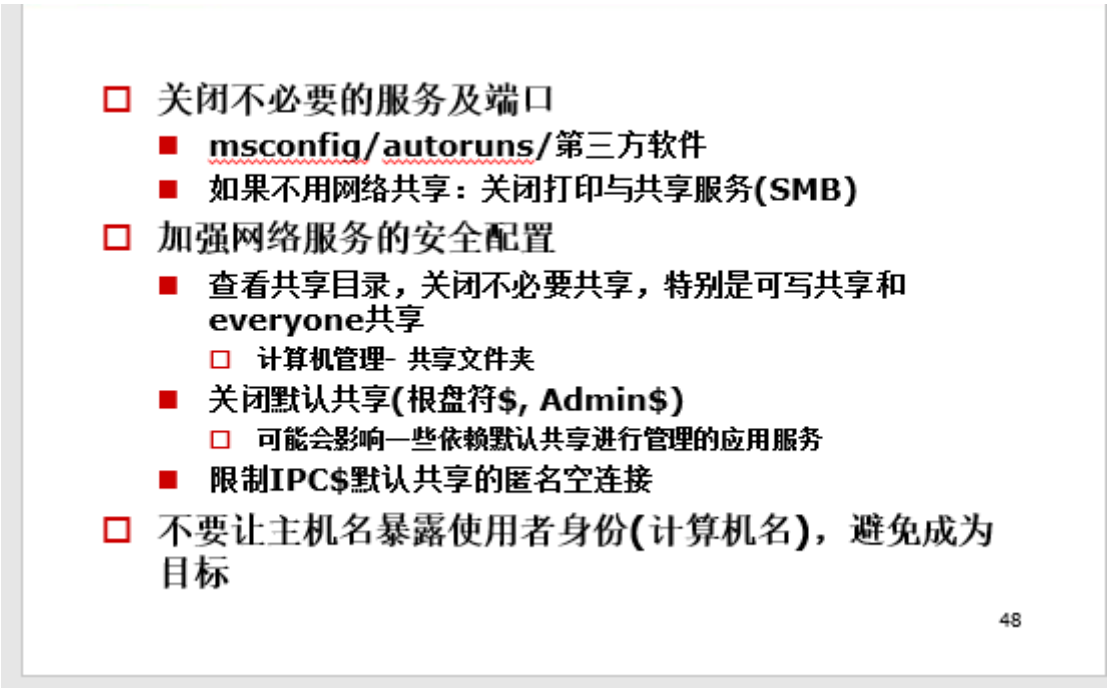
## 如何防范网络查点

1.关闭不必要的网络服务，禁止SMB空会话、共享

2.加强网络服务的安全配置：限制SMB共享、避免FTP\SMB弱口令以及匿名

3.放弃使用不安全的网络协议：telnet--->SSH、FTP

4.避免暴露身份，采用工具改变旗标信息




## 网络嗅探

利用计算机网络接口截获目的地为其他计算机的数据报文，监听网络流中所包含的用户账户密码等信息

## 如何防止网络嗅探

1.采用安全的网络拓扑，将共享式网络升级为交换式网络；交换机上设置vlan分段，分段越细越安全

2.用静态ARP或者MAC-端口映射表替代动态机制，防止MAC、ARP欺骗

3.在重要的数据传输点加强安全防范，如网关路由器交换机等

4.避免使用明文传输口令或者网络协议，telnet-ssh；IPSEC-TLS

## 流重组

将同属于一个TCP/UDP会话的IP包负载按序重新组装，还原应用层数据的过程

## 拒绝服务攻击DOS

DOS攻击是指利用网络协议漏洞或其它系统以及应用软件漏洞耗尽被攻击目标CPU、内存、带宽、磁盘等系统资源，使得被攻击的计算机网络无法正常提供服务，直至系统停止响应甚至崩溃的攻击方式

## DoS 原理

攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息。由于地址是伪造的，所以服务器一直等不到回传的消息，分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后，连接会因超时而被切断，攻击者会再度传送新的一批请求，在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。

## DOS种类

1.资源耗尽型：贷款、磁盘、cpu、内存资源

2.配置修改型：注册表

3.基于系统缺陷：口令输入过多导致账户锁定

4.物理实体破坏型

## DOS攻击的基本形式

1.服务过载

2.消息流：网络风暴

3.信号接地：关闭网络电缆接地

4.粘住攻击：tcp半开

## 应付DDoS攻击的策略

- （1）IDS的检测方法是：分析一系列的UDP报文，寻找那些针对不同目标端口，但来自于相同源端口的UDP报文。或者取10个左右的UDP报文分析那些来自于相同的源IP、相同的目标IP、相同的源端口，但不同的目标端口的报文。这样可以逐一识别攻击的来源。
- （2）寻找那些相同的源地址和相同的目标地址的ICMP Port Unreachable的信息。

## Bot

机器人(Robot)的缩写，是一段可以自动执行预先设定功能，可以被控制，具有一定人工智能的程序。通常带有恶意代码的Bot被秘密植入受控计算机，主动连接服务器接受控制指令，并依照指令完成相应功能。

## Zombie

被包含恶意代码的Bot感染或能被远程控制的计算机，又名僵尸计算机。

### 如何发现僵尸网络？

- IDS方法
  - 必须充分了解僵尸程序，提取指纹信息作为IDS检测的特征
- 行为监测法
  - 僵尸程序行为模式：快速连接控制信道、长时间在线发呆、…
- 蜜罐捕获法
  - 通过部署蜜罐对僵尸程序进行捕获—样本
  - 通过对网络行为进行监视和分析—僵尸网络控制信道信息

## DOS发展趋势

重放追踪技术升级

攻击过程日趋智能化

攻击手段日趋多样化

## Web应用程序三层架构

表示层、业务逻辑层、数据层

## 针对web不同架构的攻击

## Web服务器平台中的安全漏洞

1.数据驱动的远程代码执行安全漏洞：缓冲区溢出、格式化字符串

2.服务器功能扩展模块漏洞

3.样本文件安全漏洞

4.源代码泄露

5.资源解析攻击

## Web应用程序安全威胁类型

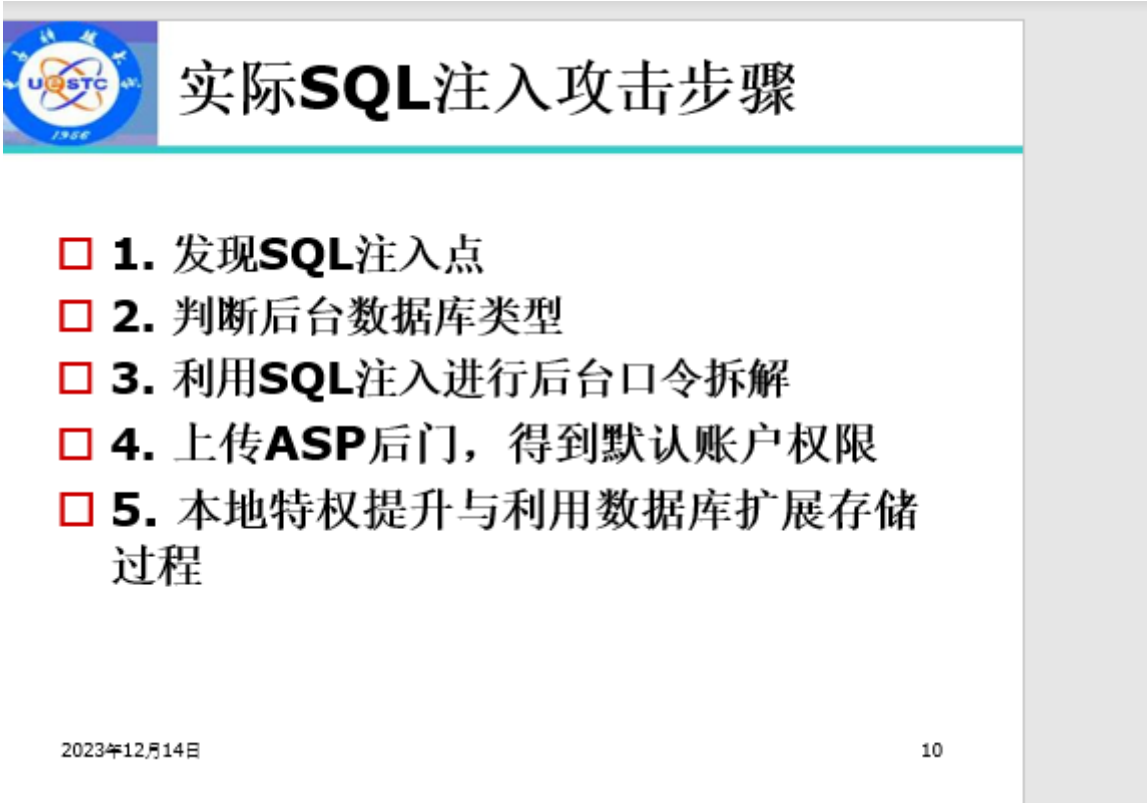
1. 针对认证机制的攻击
2. 针对授权机制的攻击
3. 客户端攻击
4. 命令执行攻击
5. 信息暴露
6. 逻辑攻击

## 攻击Web数据内容

1. 安全敏感信息泄露
2. 网站内容篡改
3. 不良信息内容上传

## 如何防范SQL注入

1. 使用类型安全的参数编码机制
2. 凡是来自外部的用户输入，必须进行完备检查
3. 将动态的SQL语句替换为存储过程、预编译SQL或ADO命令对象
4. 加强SQL数据库服务器的配置和连接




1.服务器端防范措施：限制、拒绝、净化

- 输入验证
- 输出净化：HTMLEncode（）
- 消除危险的输入点

2.客户端方案措施

- 提高浏览器安全等级
- 关闭Cookie，或者将Cookie设置为只读
- 使用安全的浏览器

## 身份认证

用户向计算机系统以一种安全的方式提交自己的身份证明，然后由系统确认用户的身份是否属实，最终决定拒绝用户或者赋予一定的权限’

## Mimikatz获取Windows密码的原理

## 口令的防护

1.选择安全密码：足够长度、大小写...

2.防止口令猜测攻击

- 硬盘分区采用NTFS格式
- 正确设置和管理账户
- 禁止不需要的服务
- 关闭不用的端口
- 禁止建立空连接

3.设置安全策略

- 强制密码历史

- 密码最长最短使用期限
- 密码长度最小值
- 密码必须符合复杂性要求

## 恶意代码

经过存储介质和网络传播，从一台PC到另外一台PC，未经授权认证破坏计算机系统完整性的程序或者代码，使得计算机按照攻击者意图执行以达到恶意目标的指令集。

## 如何防范IP源地址欺骗

1.使用随机化的初始序列号，避免远程盲攻击

2.使用网络层安全传输协议IPsec

3.避免采用基于IP地址的信任策略，以基于加密算法的用户身份认证机制来替代

4.在路由器和网关上实施包检查和过滤，入站出站过滤

5.真实源IP地址验证

## 如何防止ARP欺骗

1. 静态绑定关键主机IP地址与MAC地址映射关系
2. 使用VLAN虚拟子网细分网络拓扑
3. 加密传输数据以降低ARP欺骗攻击的危害后果
4. 使用ARP防范工具：ARP防火墙

## TCP/IP协议栈各层的安全防护

1.网络接口层：主要防护的是网路嗅探

- 监听检测
- vlan细分结构
- 关键网关防护
- 加密通信协议

2.互联层

- 检测过滤各种欺骗
- 防火墙、关键网关
- IP-MAC静态映射表、IPsec加密

3.传输层

加密传输安全控制机制：身份认证、访问控制

4.应用层

加密；认证；数字签名；https；IDS

# 802.11安全弱点

- 广播网络，共享介质
  - 没有明确的边界：无法有效控制
  - 介质共享(无线电波)：信道抢占DoS攻击、报文窃听注入
  - 很难探知窃听/发送点的位置：难以追溯攻击
- 802.11安全威胁
  - 窃听：如果不加密/弱加密，存在数据窃听风险
  - 注入：报文易于造假，随意注入共享介质
  - 信道抢占/干扰：电波频道抢占、电磁干扰
  - 身份假冒：破解口令之后可假冒身份进入网络



# WiFi加密方式

- 不加密-开放网络
- WEP
  - RC4流加密算法, 明文初始化向量, CRC32校验
  - 存在设计缺陷，极易破解
- WPA/WPA2
  - WPA: TKIP(RC4+rekeying)临时过渡方案
  - WPA2: 802.11i(AES/CCMP)
  - 预先共享密钥（WPA-PSK/WPA-PSK2）
  - 外部身份认证服务(Radius, WPA enterprise)
  - 802.1x身份认证机制



## 工具

DNS注册信息Whois查询（3R信息）：SamSpade, SuperScan

DNS查询域名映射工具：nslookup/dig

Whois客户程序： IP whois查询

网络入侵检测系统/网络入侵防御系统: Snort

网络路由侦察：：traceroute/tracert 虚假响应信息: RotoRouter

nmap（nmap FE, Zenmap）、Superscan：扫描

| 技术类型 | 经典工具 |
| --- | --- |
| 操作系统主动探测技术 | nmap -O, queso |
| 操作系统被动辨识技术 | P0f, siphon |
| 网络服务主动探测技术 | nmap -sV, |
| 网络服务被动辨识技术 | PADS |
| 系统扫描检测工具 | scanlogd, PortSentry, Genius |
| 网络入侵检测系统: | Snort中的portscan检测插件 |
| UDP端口扫描 | udp-scan nmap wups scanline: |
| 主机扫描监测工具 | Scanlogd |
| 扫描 | nmap（nmap FE, Zenmap）、Superscan |
| 被动操作系统识别技术流量监听(开放端口): | tcpdump |
| 网络服务特征被动匹配和识别 | PADS |
| 网络服务旗标抓取和探测 | nmap -sV |
| 漏洞扫描 | ISS、SATAN、Nessus、Xscan（冰河黄鑫）、OpenVAs Greenbone |
| 网络查点：网络服务旗标抓取 | telnet netcat |
| 查点 | net view\nbtscan\nltest\nbtstat |
| 网络嗅探 | wireshark, Sniffer Pro，BPF/libpcap，NPF/WinpcapSnort\、dsniff、sniffit和linux_sniffernNPF/winpcap/windumpnSnifferPronButtsniffer、NetMon、Network Associates Sniffer |
| 抓包 | Tcpdump |
| 网络流重组 | nstreams, snort |

| 技术类型 | 经典工具 |
| --- | --- |
| 高层统计和摘要分析 | Netflow, RRDTools |
| Web应用安全辅助分析工具 | Burp Suite，Fiddler，WebScarab，，Paros Proxy和SPIKE Proxy |
| 结合爬虫的评估与漏洞探测工具 | Whisker与Libwhisker / Nikto / N-Stealth |
| 黑客渗透测试工具 | NBSI、HDSI、Domain |
| 商业Web应用安全评估系统和漏洞扫描器 | Nessus、IBM - Appscan、HP WebInspect、WVS、极光、Jsky |
| 自动化SQL注入漏洞发现 | Wposion、nmieliekoek.pl |
| 自动化SQL注入测试 | SPIKE Proxy工具nSPI Toolkit工具包中的“SQL Injector”工具 |
| 国内sql黑客界工具 | NBSI、HDSI、阿D注入工具、CSC、WED...、Pangolin |
| 网马 | CHM网马、Icefox冰狐、MS06-014网马, ANI网马：熊猫烧香 |
| 网页木马追踪和定位系统 | MwHunter |
| 网页木马、植入恶意代码采集系统 | MwFetcher |
| 常用的口令获取及破解工具 | L0phtcrack、Mimikatz、NTSweep、NTCrack、PWDump……Rainbow tables、Mimikatz |
| 病毒 | CIH、Melissa |
| 蠕虫 | ILOVEYOU、Code Red、SQL Slammer、WORM_LOVGATE.AE、PE_LOOKED.ID-O |
| 木马 | QAZ、冰河，NetBull、广外女生、蓝色火焰 |
| 恶意代码工具 | TCP View、Regmon、Filemon、InstallRite |
| 后门 | 灰鸽子 |
| 原始报文伪造技术 | Libnet库 for C、Scapy库 for Pythono、Netwox/Netwag |
| IP源地址欺骗 | Netwox、Nmap |
| 无线踩点软件 | NetStumbler、Kismet |

| 技术类型 | 经典工具 |
| --- | --- |
| Aircrack-ng 破解WEP密钥 | Aircrack-ng |
| oWindows平台无线Sniffer软件 | OmniPeek Personal WinAirCrack/Airodump |
| | |
| | |
| | |