

04

信息安全抗攻击技术



DOS拒绝服务攻击

- ◆ 为对抗攻击者的攻击， 密钥生成需要考虑3个方面的因素： 增大密钥空间、选择强钥 (复杂的)、 密钥的随机性 (使用随机数) 。
- ◆ 拒绝服务攻击有许多种， 网络的内外部用户都可以发动这种攻击。内部用户可以通过长时间占用系统的内存、CPU 处理时间使其他用户不能及时得到这些资源，而引起拒绝服务攻击；外部黑客也可以通过占用网络连接使其他用户得不到网络服务。
- ◆ 外部用户针对网络连接发动拒绝服务攻击主要有以下几种模式： 消耗资源、破坏或更改配置信息、物理破坏或改变网络部件、利用服务程序中的处理错误使服务失效。
- ◆ 分布式拒绝服务DDoS攻击是传统DoS攻击的拓展， 攻击者首先侵入并控制一些计算机，然后控制这些计算机同时向一个特定的目标发起拒绝服务攻击。克服了传统DOS受网络资源的限制和隐蔽性两大缺点。



DOS拒绝服务攻击

◆ 拒绝服务攻击的防御方式

(1) 加强对数据包的特征识别，攻击者发送的数据包中是有一些特征字符串。通过搜寻这些特征字符串，就可以确定攻击服务器和攻击者的位置。

设置防火墙监视本地主机端口的使用情况。如果发现端口处于监听状态，则系统很可能受到攻击。

对通信数据量进行统计也可获得有关攻击系统的位置和数量信息。在攻击时，攻击数据的来源地址会发出超出正常极限的数据量。

尽可能的修正已经发现的问题和系统漏洞



ARP欺骗

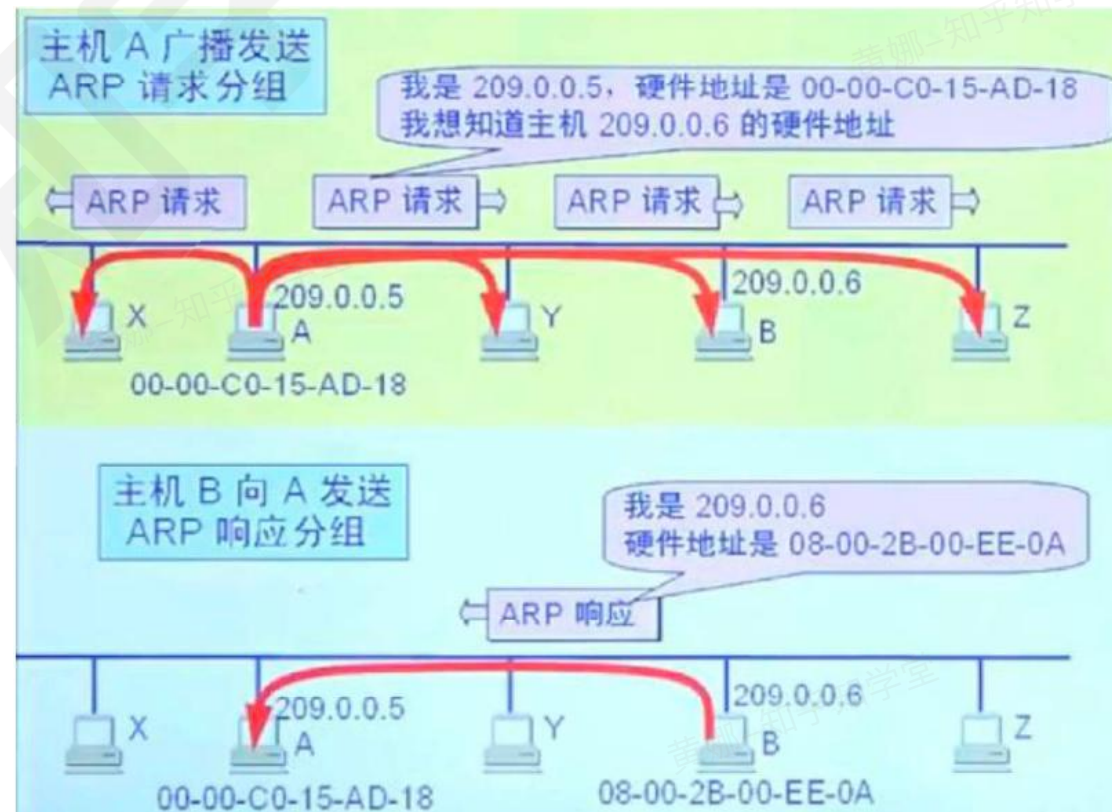
◆ 正常ARP原理：

如图所示，主机A想知道局域网内主机B的MAC地址，那么主机A就广播发送ARP请求分组，局域网内主机都会收到，但只有B收到解析后知道是请求自己的MAC地址，所以只有B会返回单播的响应分组，告诉A自己的MAC地址。

A收到响应分组后，会建立一个B的IP地址和MAC地址映射，这个映射是动态存在的，如果一定时间AB不再通信，那么就会清空这个地址映射，下次如果还要通信，则重复这个过程。

◆ ARP欺骗原理：

上述过程主机A是不管其有没有发送过请求广播分组的，而是只要收到了返回的分组信息，就会刷新IP和MAC地址的映射关系，这样就存在安全隐患，假设有主机C，模拟返回分组格式，构造正确的IP地址和自己的MAC地址映射，A收到后也会刷新映射关系，那么当A再次向B发送信息时，实际就发送到了的MAC地址，数据就被C监听到了。





ARP欺骗

◆ ARP欺骗的防范措施:

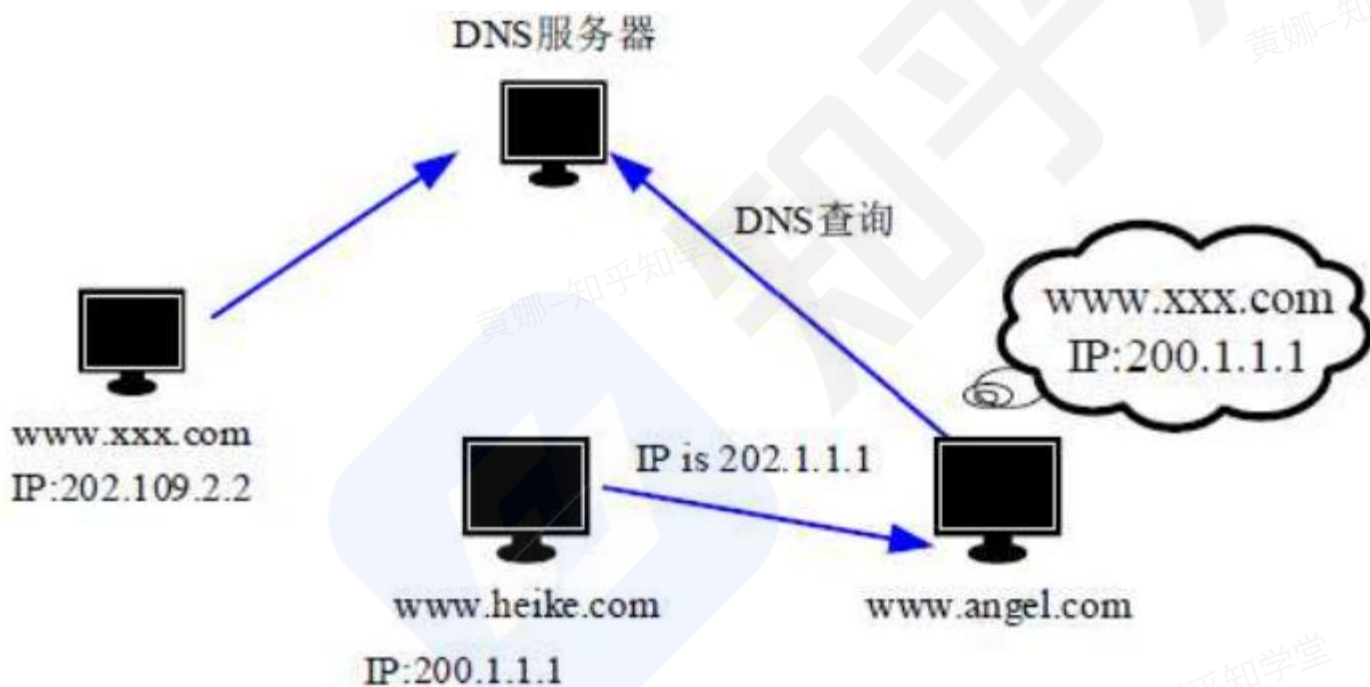
- ① 在winxp下输入命令：`arp-s gate-way-ip gate-way-mac` 固化arp表，阻止arp欺骗
- ② 使用ARP服务器。通过该服务器查找自己的ARP 转换表来响应其他机器的ARP广播。确保这台ARP服务器不被黑。
- ③ 采用双向绑定的方法解决并且防止ARP欺骗。
- ④ ARP 防护软件——ARPGuard 。通过系统底层核心驱动，无须安装其他任何第三方软件（如WinPcap），以服务及进程并存的形式随系统启动并运行，不占用计算机系统资源。无需对计算机进行 IP地址及MAC地址绑定，从而避免了大量且无效的工作量。也不用担心计算机会在重启后新建ARP 缓存列表， 因为此软件是以服务与进程相结合的形式存在于计算机中，当计算机重启后软件的防护功能也会随操作系统自动启动并工作 。



DNS欺骗

◆ DNS 欺骗原理:

首先是冒充域名服务器，然后把查询的IP 地址设为攻击者的IP地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了。也即改掉了域名和IP地址的对应关系。黑客是通过冒充DNS服务器回复查询IP的，如下图所示：





DNS欺骗

◆ DNS 欺骗的检测：

- ① **被动监听检测**：通过**旁路监听的方式**，捕获所有DNS请求和应答数据包，并为其建立一个请求应答映射表。如果在一定的时间间隔内，**一个请求对应两个或两个以上结果不同的应答包**，则怀疑受到了DNS欺骗攻击。
- ② **虚假报文探测**：采用**主动发送探测包**的手段来检测网络内是否存在DNS欺骗攻击者。如果向一个**非DNS服务器发送请求包**，正常来说不会收到任何应答，如果收到了应答包，则说明受到了攻击。
- ③ **交叉检查查询**：在客户端收到DNS应答包之后，向DNS服务器**反向查询**应答包中返回的IP地址所对应的DNS名字，如果二者一致说明没有受到攻击，否则说明被欺骗。



IP欺骗

◆ IP欺骗的原理和流程：

- ① 首先使被冒充主机host b 的网络暂时瘫痪，以免对攻击造成干扰；
- ② 然后连接到目标机host a 的某个端口来猜测ISN 基值和增加规律；
- ③ 接下来把源地址伪装成被冒充主机host b，发送带有SYN标志的数据段请求连接；
- ④ 然后等待目标机host a 发送SYN+ACK 包给已经瘫痪的主机，因为现在看不到这个包；
- ⑤ 最后再次伪装成主机host b向目标主机host a 发送的ACK，此时发送的数据段带有预测的目标机的ISN+1；
- ⑥ 连接建立，发送命令请求。

◆ IP欺骗的防范：

预防这种攻击可以删除UNIX中所有的/etc/hosts.equiv、\$HOME/.rhosts 文件，修改/etc/inetd.conf 文件，使得RPC机制无法应用。另外，还可以通过设置防火墙过滤来自外部而信源地址却是内部IP的报文。



端口扫描

◆ **端口扫描**就是**尝试与目标主机的某些端口建立连接**，如果目标主机该端口**有回复**（见三次握手中的第二次），则说明该**端口开放**，即为“活动端口”。

◆ 扫描原理分类：

① **全TCP连接**。这种扫描方法使用三次握手，与目标计算机建立标准的TCP连接。

② **半打开式扫描 (SYN 扫描)**。在这种扫描技术中，扫描主机自动向目标计算机的指定端口**发送SYN数据段**，**表示发送建立连接请求**。

- 如果目标计算机的回应TCP报文中**SYN=1 ACK=1**，则说明该端口是**活动的**，接着扫描主机传送一个RST给目标主机拒绝建立TCP 连接，从而导致三次握手的过程失败。
- 如果目标计算机的**回应是RST**，则表示该端口为“**死端口**”，这种情况下，扫描主机不用做任何回应。

③ **FIN 扫描**。依靠**发送FIN来判断目标计算机的指定端口是否是活动的**。发送一个**FIN=1 的TCP 报文**到一个关闭的端口时，该报文会被丢掉，并返回一个**RST 报文**。但是，如果当 FIN 报文到一个**活动的端口时**，该报文只是被简单的丢掉，**不会返回任何回应**。从FIN 扫描可以看出，这种扫描没有涉及任何TCP 连接部分。因此，这种扫描比前两种都安全，可以称之为秘密扫描。

④ **第三方扫描**。第三方扫描又称“**代理扫描**”，这种扫描是利用**第三方主机来代替入侵者进行扫描**。这个第三方主机一般是入侵者通过入侵其他计算机而得到的，该“第三方”主机常被入侵者称之为“**肉鸡**”。这些“肉鸡”一般为安全防御系数极低的个人计算机。



DOS拒绝服务攻击

◆ 强化TCP/IP堆栈以抵御拒绝服务攻击

- ① **同步包风暴(SYN Flooding)**：利用TCP协议缺陷发送大量伪造的TCP连接请求，使得被攻击者资源耗尽。三次握手，进行了两次，不进行第三次握手，连接队列处于等待状态，大量这样的等待，会占满全部队列空间，使得系统挂起。可以通过修改注册表防御SYN Flooding 攻击。
- ② **ICMP 攻击**。ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。比如，前面提到的" **Ping of Death** "攻击就是利用操作系统规定的ICMP 数据包的最大尺寸不超过 64KB 这一规定，达到使TCP/IP 堆栈崩溃、主机死机的效果。可以通过改注册表防御ICMP攻击：
- ③ **SNMP攻击**。SNMP 还能被用于控制这些设备和产品，重定向通信流，改变通信数据包的优先级，甚至断开通信连接。总之，入侵者如果具备相应能力，就能完全接管你的网络。可以通过修改注册表项防御。

系统漏洞扫描指对重要计算机信息系统进行检查，发现其中可能被黑客利用的漏洞。包括**基于网络的漏洞扫描**（通过网络远程扫描主机）、**基于主机的漏洞扫描**（在目标系统安装了代理扫描）。

考试真题

SYN Flooding攻击的原理是()。

- A. 利用TCP三次握手，恶意造成大量TCP半连接，耗尽服务器资源，导致系统拒绝服务
- B. 操作系统在实现TCP/IP协议栈时，不能很好地处理TCP报文的序列号紊乱问题，导致系统崩溃
- C. 操作系统在实现TCP/IP协议栈时，不能很好地处理IP分片包的重叠情况，导致系统崩溃
- D. 操作系统协议栈在处理IP分片时，对于重组后超大的IP数据包不能很好地处理，导致缓存溢出而系统崩溃

答案：A