选择

1、在网络安全中，截取是指未授权的实体得到了资源的访问权，这是对（ ）。
A、可用性的攻击
B、完整性的攻击
C、保密性的攻击
D、真实性的攻击
2、TCP 首部中建立连接的同步标志位是（ ）。
A、FIN
B、ACK
C、SYN
D、RST
3、下面关于防火墙系统的功能说法不正确的是（ ）。
A、保护了内部安全网络不受外部不安全网络的侵害
B、决定了外部的哪些人可以访问内部服务
C、决定了那些内部服务可以被外部访问
D、由于有防火墙的保护，内部人员可以放心地访问外部的任何服务
4、在 IP 互联网层提供安全的一组协议是（ ）。(5.0 分)
A、TLS
B、SSH
C、PGP
D、IPSec
5、以下哪种协议不是链路层协议（ ）。
A、ICMP
B、IEEE802.3
C、PPP
D、SLIP
6、虚拟专网 VPN 使用（ ）来保证信息传输中的保密性。
A、IPSec
B、隧道
C、（A）和（B）
D、以上都不正确
7、下面不属于木马伪装手段的是（ ）。
A、自我复制
B、隐蔽运行
C、捆绑文件
D、修改图标
8、在使用 super scan 对目标网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是什么（ ）。(5.0 分)
A、文件服务器
B、邮件服务器
C、WEB 服务器

D、DNS 服务器
9、以下是 DoS 攻击手段的是（ ）。(5.0 分)
A、ping flooding
B、IP 地址欺骗
C、ARP 欺骗
D、泪滴攻击
10、防止用户被冒名所欺骗的方法是（ ）。(5.0 分)
A、对信息源发方进行身份验证
B、进行数据加密
C、对访问网络的流量进行过滤和保护
D、采用防火墙
11、按照检测数据的来源可将入侵检测系统（IDS）分为（ ）。(5.0 分)
A、基于主机的 IDS 和基于网络的 IDS
B、基于主机的 IDS 和基于域控制器的 IDS
C、基于服务器的 IDS 和基于域控制器的 IDS
D、基于浏览器的 IDS 和基于网络的 IDS
12、加密技术不能实现（ ）。(5.0 分)
A、数据信息的完整性
B、基于密码技术的身份认证
C、机密文件加密
D、基于 IP 头信息的包过滤
13、DDoS 攻击的是目标的（ ）。(5.0 分)
A、机密性
B、完整性
C、可用性
D、不可抵赖性
14、以下哪些不是网络安全保护的目标（ ）。(5.0 分)
A、完整性
B、机密性
C、可控性
D、连通性
15、当你感觉到你的 Windows 操作系统运行速度明显减慢，当你打开任务管理器后发现 CPU 的使用率达到了百分之百，你最有可能认为你受到了哪一种攻击（ ）。(5.0 分)
A、特洛伊木马
B、拒绝服务
C、欺骗
D、中间人攻击
16、下面关于防火墙的缺陷叙述错误的是（ ）。(5.0 分)
A、限制有用的网络服务
B、无法保护内部网络用户的攻击
C、无法保护外部网络用户的攻击
D、无法防备新的网络安全问题
17、以下关于非对称密钥加密说法正确的是（ ）。(5.0 分)
A、加密方和解密方使用的是不同的算法

B、加密密钥和解密密钥是不同的
C、加密密钥和解密密钥匙相同的
D、加密密钥和解密密钥没有任何关系
18、入侵检测的一般步骤不包括（ ）。(5.0 分)
A、信息收集
B、信息分析
C、结果处理
D、信息传输
19、以下哪种攻击手段不是 DoS 攻击（ ）。(5.0 分)
A、ARP 欺骗
B、ping of death
C、smurf
D、SYN flooding
20、以下哪个系列的协议是 WLAN 协议（ ）。(5.0 分)
A、802.15
B、802.11
C、802.16
D、802.20
21、TCP 建立连接的三次握手中第三次握手标志位设置正确的是（ ）。(5.0 分)
A、SYN=0,ACK=0
B、SYN=0,ACK=1
C、SYN=1,ACK=0
D、SYN=1,ACK=1
22、DNS 是哪一层的协议（ ）。(5.0 分)
A、应用层
B、传输层
C、网络层
D、数据链路层
23、交换机是哪一层设备（ ）。(5.0 分)
A、应用层
B、传输层
C、网络层
D、数据链路层
24、网桥是哪一层设备（ ）。(5.0 分)
A、应用层
B、传输层
C、网络层
D、数据链路层
25、路由器是哪一层设备（ ）。(5.0 分)
A、应用层
B、传输层
C、网络层
D、数据链路层
26、第三层交换机是哪一层设备（ ）。(5.0 分)

A、应用层
B、传输层
C、网络层
D、数据链路层
27、以下不是垃圾邮件产生的主要原因的是（ ）。(5.0 分)
A、技术缺陷
B、缺乏相关的法律约束
C、利益诱惑
D、管理缺陷
28、网络侦听是一种（ ）的技术。(5.0 分)
A、应用层
B、传输层
C、网络层
D、数据链路层
29、VPN 在网络层可以用（ ）来实现。(5.0 分)
A、IPSec
B、SSL
C、MPLS
D、VLAN
30、VPN 在传输层可以用（ ）来实现。(5.0 分)
A、IPSec
B、SSL
C、MPLS
D、VLAN
31、IPSec 工作在（ ）。(5.0 分)
A、应用层
B、传输层
C、网络层
D、数据链路层
32、SSL 工作在（ ）。(5.0 分)
A、应用层
B、传输层
C、网络层
D、数据链路层
33、以下哪个选项不是无线局域网结构模式（ ）。(5.0 分)
A、Infrastructure 模式
B、P2P 模式
C、混和模式
D、Ad Hoc 模式
34、以下关于拒绝服务攻击的特点描述错误的是（ ）。(5.0 分)
A、易于实现
B、难于防范
C、破坏可靠性
D、难于追查

35、拒绝服务攻击造成的危害不包括（ ）。(5.0 分)
A、破坏网络或系统的可靠性
B、经济损失
C、破坏网络或系统的可用性
D、信誉损失

填空

1.将网卡设置在_____模式下，就可以捕获流经网卡的数据包。
混杂（杂错）

2.通过修改 MAC 地址的方法发起的攻击叫做_____。
MAC 地址欺骗

3.从技术上划分，入侵检测系统有两种模型 _____和_____。
异常检测　　滥用检测

4.木马程序一般由两部分组成，分别是_____和_____。
控制端　　被控制端

5.IPSec 在 Internet 的_____层提供安全服务，为_____提供了安全保障。
网络层　　私有信息通过公众网络

6.查看本机 IP 地址的命令是_____，查看本机开放端口的命令是_____，查看远程主机连通性的命令是_____。
ipconfig　　netstat　　ping

7.P2DR 模型是一种常用的网络安全模型，包括四个主要部分 _____、_____、_____和_____。
安全策略　　防护　　检测　　响应

8.一个完善的 DDoS 攻击体系包括 _____、_____、_____和_____。
攻击者　　主控端　　代理端　　被攻击者

9.无线网络中的 AP 是指_____。
无线接入点

10.网络的基本功能有_____、_____和_____。
资源共享　　通信　　远程控制

11.导致网络安全威胁的原因不外乎以下三个_____、_____和_____。

系统的开放性　系统的复杂性　人的因素

12. 802.11 协议是_____组织的标准，在 802.11 协议中定义了两种类型的设备，分别是_____和_____。

IEEE　无线终端　无线接入点

13.计算机蠕虫包括三个模块 _____、_____和_____。

扫描模块　感染模块　执行功能模块

14.802.11 协议的 MAC 层采用的介质访问控制方法是_____。

CSMA/CA

15.IPsec 有两种工作模式，分别是_____和_____。

传输模式　隧道模式

16.NAT 有三种类型 _____、_____和_____。

静态 NAT　NAT 池　端口 NAT（PAT）

17.IPSec 定义的两种通信保护机制分别是_____机制和_____机制。

AH　ESP

18.木马传播的方式主要有两种 _____和_____。

E-mail　软件下载

19.垃圾邮件从内容上主要分为_____和_____。

广告邮件　宣传邮件

20.以太网环境有_____和_____两种基本类型。

共享以太网　交换以太网

21._____和_____可用于嗅探交换机上的通信。

ARP 欺骗　MAC 泛滥

22.应用层常见的攻击模式有_____、_____和_____。

带宽攻击　缺陷攻击　控制目标主机

23.IPSec 工作在_____层，SSL 工作在_____层，MPLS 工作在_____层。

网络层　传输层　应用层

24.无线局域网的结构有_____、_____和_____三种模式。

Infrastructure 模式　Ad Hoc 模式　混和模式

25.　802.11 协议中定义了两种类型的设备，分别是_____和_____。

无线终端　　接入点

26.以太网络的介质访问控制方法是_____，无线局域网 802.11 协议的介质访问控制方法是_____。

CSMA/CD　　CSMA/CA

27.无线局域网有_____、_____和_____安全需求。

数据机密性　　数据完整性　　访问控制

28.入侵检测系统按照检测的数据来源可以分为_____和_____两种。

HIDS　　NIDS

29.入侵检测系统根据工作方式可分为_____和_____。

离线检测　　在线检测

30.异常检测技术的误警率比滥用检测_____，漏警率比滥用检测_____。

高　　低

31.防火墙与 IPS 联动的方式有_____和_____。

通过开放接口实现联动　　通过紧密集成实现联动

32.IPS 根据部署方式可以分为 3 类，分别是_____、_____和_____。

NIPS　　HIPS　　AIPS

33.拒绝服务攻击具有_____、_____、_____等特点。

易于实现　　难于防范　　难于追查

34.拒绝服务攻击的危害主要体现在_____、_____、_____。

破坏网络或系统的可用性　　经济损失　　信誉损失

35.DDoS 攻击的过程是_____、_____、_____。

搜集目标信息　　占领傀儡机　　实际攻击

36.DDoS 的攻击防御中，最关键的技术是如何分辨_____和_____。

合法业务流量　　恶意业务流量

名词解释

1. **异常检测技术**
   异常检测的假设是任何一种入侵行为都能由于其偏离正常或所期望的系统和用户的活动规律而被检测出来
2. **误用检测（滥用检测）**
   一种基于模式匹配的网络入侵检测技术，将搜集到的信息与已知的网络入侵和系统误用模式数据库进行比较，即可发现未知的网络攻击行为
3. **TCP 半连接**
   在三次握手过程中，服务器发送 SYN-ACK 之后，收到客户端的 ACK 之前的 TCP 连接称为半连接
4. **VPN**
   是公司内部或者不同公司和组织之间为了在广域网上进行通信而建立的私有通信网络
5. **DMZ（非军事化区）**
   为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区
6. **僵尸网络**
   计算机被病毒感染后，随时按照黑客的指令展开拒绝服务攻击或发送垃圾信息，（用户毫不知情，仿佛没有自主意识的僵尸）这样的计算机达到一定数量后，形成一个庞大的网络
7. **泪滴攻击**
   IP 数据包在网络传递时，数据包可以分成更小的片段，攻击者可以通过发送两端或更多数据包实现泪滴攻击
8. **IP 地址欺骗**
   攻击者假冒他人 IP 地址，发送数据包
9. **交换机失败保护模式**
   交换机所处特殊模式，交换机维护 IP 地址和 MAC 地址的映射关系时会花费一定处理能力，网络通信出现大量虚假 MAC 地址时，某些类型的交换机会出现过载情况，从而转化到失败保护模式，工作方式和集线器相同
10. **零日漏洞**
    指被发现后立即被恶意利用的安全漏洞，能造成巨大破坏
11. **木桶理论**
    整个系统防护能力，取决于系统中安全防护能力最薄弱的环节
12. **DDOS 攻击**
    是目前企业网络和电信网系统面临最主要攻击类型之一，要么大数据、大流量压垮网络设备和服务器，要么有意制造大量无法完成的不完全请求来快速耗尽服务器资源
13. **TCP SYN 扫描**
    通常是“半开放扫描，扫描端收到 ACK/SYN 应答时，发送了一条拒绝建立连接的 RST 请求，目标端不会将其记录在日志中”

简答

1.什么是 IP 地址扫描

利用 ICMP 的回应请求与应答报文，运用 ping 探测目标地址，对此作出响应，表示其存在。

2.简述 CSMA/CA 的工作流程

先听后发，边发边听，冲突停发，随机延迟后重发。
（ 发送数据前 先侦听信道 du 是否空闲 ,若空闲，则立即发送数据。若信道忙碌，则等待一段时间至信道中的信息传输结束后再发送数据；

若在上一段信息发送结束后，同时有两个或两个以上的节点都提出发送请求，则判定为冲突。若侦听到冲突,则立即停止发送数据，等待一段随机时间,再重新尝试。）

3.什么是 TCP SYN 攻击

攻击主机伪造源 IP 地址，向目标主机的特定 TCP 端口发送许多 SYN 包，目标主机回复确认包，由于源地址是不存在的，目标主机需要不断地重发直至超时，伪造的 SYN 包将长时间占用连接队列，正常的 SYN 请求被丢弃，导致目标主机内存资源不断消耗，直至枯竭。

4.计算机病毒与蠕虫的区别

（1）存在形式：蠕虫是独立的程序；计算机病毒是寄生于宿主文件的。
（2）攻击目标：蠕虫感染网络；计算机病毒攻击本地文件。
（3）主动性：蠕虫主动攻击；计算机病毒随着宿主而运行。

5.无限局域网的安全需求有哪些

（1）数据机密性：对传输数据进行加密。
（2）数据完整性：防止空中传输的数据遭到非授权

6.什么是泪滴攻击

将 IP 数据包分成很多小片段，通过发送伪造的相互重叠的数据包，使其难以被接收主机重新组合，造成资源缺乏甚至机器重启。

7.Smurf 攻击的原理是什么

攻击者向网络广播地址发送 ICMP 包,并将回复地址设置成目标网络的广播地址,通过使

用 ICMP 应答请求数据包来淹没目标主机的方式进行,最终导致该网络的所有主机都对次 ICMP 应答请求作出答复,导致网络阻塞。

8.简述计算机蠕虫的组成

（1）扫描模块：探测目标主机。
（2）感染模块：感染目标计算机。
（3）功能执行模块：执行蠕虫设计者预定义的功能。

9.简述共享密钥的认证过程

①客户端发送一个认证请求 Authentication Request 给无线接入点要求进行共享密钥认证
②无线接入点回复一个认证响应信息 Authentication Response,包含挑战信息;
③客户端使用本地配置的 WEP 密钥加密挑战信息,然后回复一个认证请求;
④无线接入点解密收到的认证信息,如果得到最初的挑战信息,然后回复一个认证响应信息同意客户接入。

10.虚拟机技术怎么防病毒

让一个物理平台同时运行多个操作系统，避免病毒导致单一应用崩溃对整个系统的影响，增强可迁移性。利用主流虚拟机技术如：虚拟硬件模式，虚拟操作系统模式和 Xen 模式等，以及运用 VT 技术。

11.VLAN 中涉及哪些协议，协议的作用是什么？

交换链路内协议（ISL）:给 VLAN 做标记，维护交换机和路由器间的通信流量；
VLAN 中继协议（VTP）:做 VLAN 同步，管理在同一个域的网络范围内 VLANs 的建立、删除和重命名，让其自动同步。

12.网络侦听的原理是什么

利用共享式的网络传输介质，将网卡设置为混杂模式，并利用数据链路访问技术来实现对网络的侦听。

13.DDos 攻击主要有哪两种手段

（1）用大数据，大流量来压垮网络设备和服务器。
（2）有意制造大量无法完成的不完全请求来快速耗尽服务器资源。

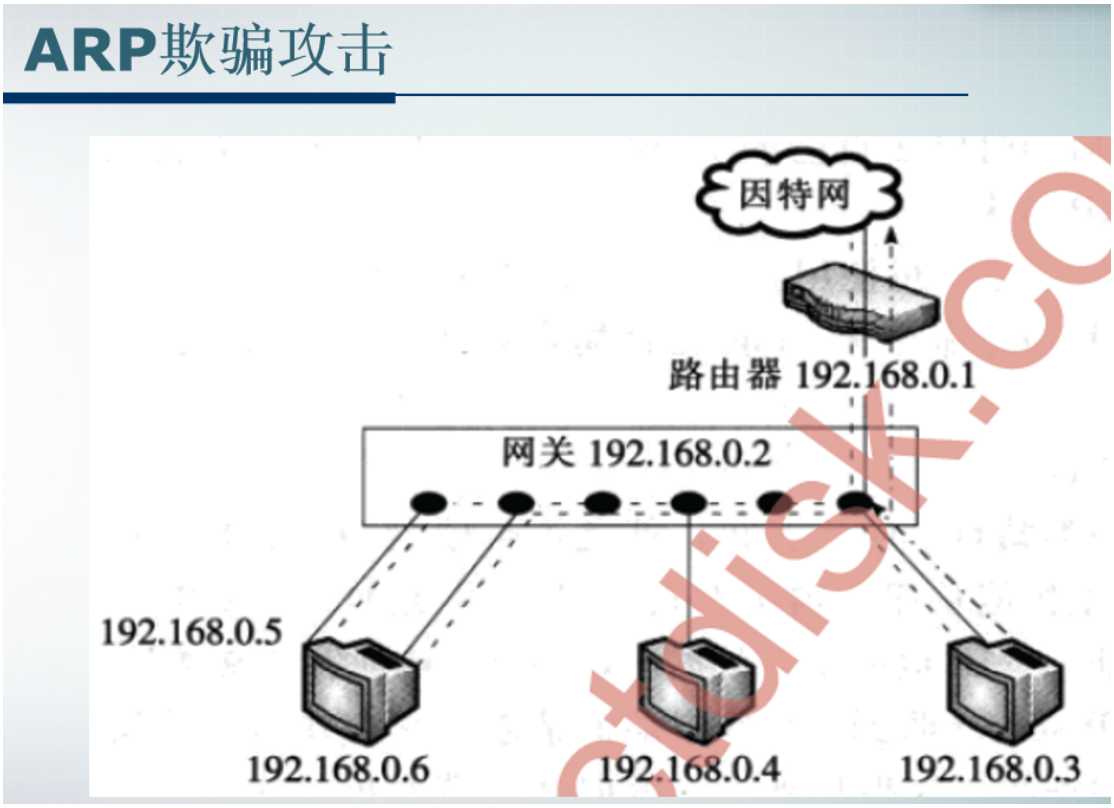
应用/简答

1. Base64 编码：
（3*8 -> 4*6）
e.g: 输入： abc
转换 ascll 码：97 98 99
转换二进制：01100001|01100010|01100011
重新组合成 4 组 6 位：011000|010110|001001|100011
每组前面用 0 补全 8 位：00011000|00010100|00001001|00100011
二进制转十进制：24 20 9 35
对应下表转换：YWJj

Table 1: The Base64 Alphabet

索引	对应字符	索引	对应字符	索引	对应字符	索引	对应字符
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v		
14	O	31	f	48	w		
15	P	32	g	49	x		
16	Q	33	h	50	y		

2. ARP 欺骗的过程简介：



攻击者主机需要用两张网卡（0.5/0.6）接入交换机的两个端口，并具有转发 IP 数据包的能力。

主机 A 想要与网关通信，广播发送 ARP 请求，攻击者迅速拦截

用网卡 1 伪造网关地址向被攻击者发送 ARP 请求包，把自己伪装成主机 A 的网关，

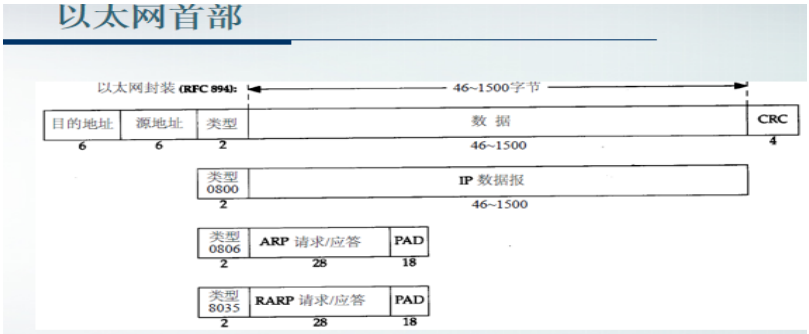
另一边用网卡 2 伪造主机地址向网关发送 ARP 请求包，把自己伪装成被攻击主机，

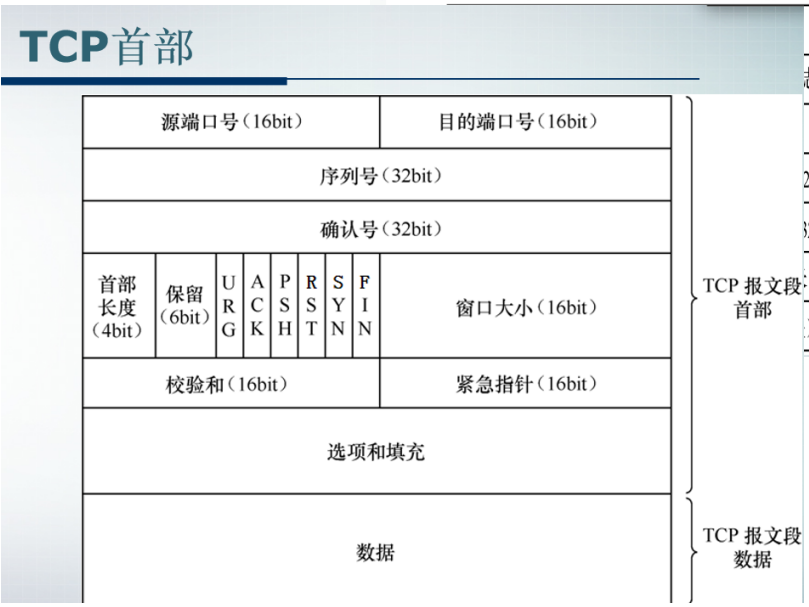
将错误的 MAC 地址和 IP 映射更新到网卡和目标主机上，

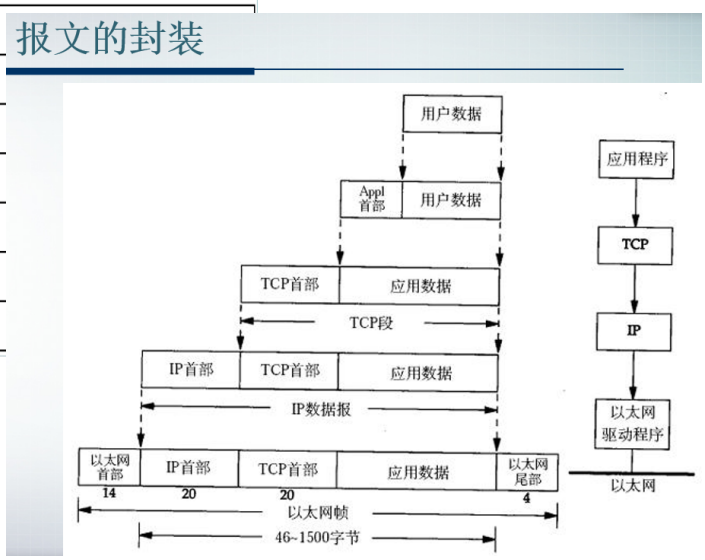
使自己成为两者通讯之间的中间人，转发和处理两者之间的数据，

起到同时欺骗目标主机和网关的目的。

3. 数据帧的解读：







4. IP 源路由攻击：

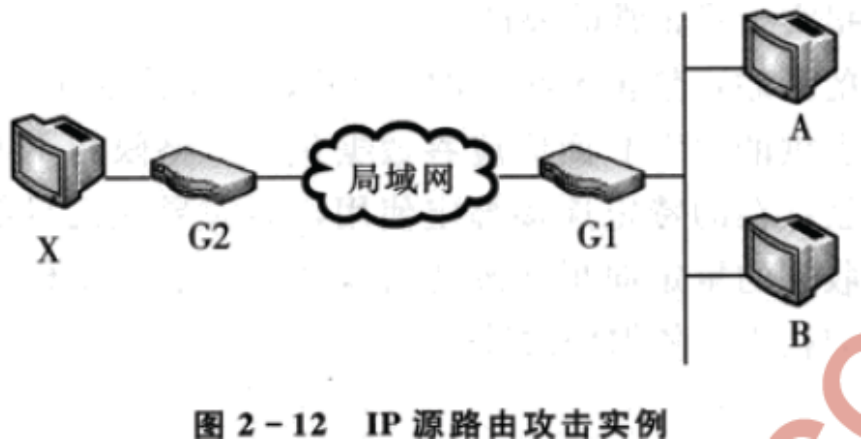


图 2－12　IP 源路由攻击实例

现有主机 A 是主机 B 的被信任机，X 想要冒充 A 从 B 获得某些服务。

1: 修改距离 X 最近的路由器 G2 将包含 B 目的地址的数据包将 X 所在网络作为目的地

2: 利用 IP 欺骗，将数据包的源地址改为主机 A 的地址并向主机 B 发送带有源路由选项的数据包。

３：B 回送数据包时根据数据包的源路由选项反转使用源路由，向 G２发送

４：G２收到数据包后根据 X 事先修改的路由表向 X 所在网络转发数据包

5：自此，X 即可在其局域网上侦听并收取 B 的数据包。

源径路由就是数据发送的主句能要求目标主机回复报文所经过的路径。发送主机在发送数据的同时指定了目标主机回复信息经过的路径。入侵者可以将自己的主机添加到路由表中，然后向目标主机发送伪造的路由信息，让目标主机发源路径回复。这样目标主机的回复信息就按照这个路径经过入侵者的路由器，入侵者就可以从目标路由器中窃听信息了。

5. NAT 的工作过程：

NAT 即网络地址转换，内网使用内部地址通过 NAT 转换成合法的 IP 地址并在 Internet 上使用。

NAT 有三种类型：

静态 NAT：内网主机与外网某个合法地址一对一对应映射

NAT 池：在外网中定义一系列合法地址动态分配映射到内部网络

端口 NAT（PNAT）：内部网络地址映射到外部网络的一个 IP 地址的不通关端口。

过程：内网主机 A 与外部网络主机 B 通讯，源 ip 为 A 的内网地址，目的 IP 为主机 B 的外网地址，到网络边界通过 NAT 技术将源 IP 转换为主机 A 映射的某外网合法地址，目的 IP 不变，主机 B 收到并回复消息时，将主机 A 映射的某外网合法地址作为目的 IP 地址，主机 B 的外网地址为源 IP 地址，主机 A 所在的局域网的网络边界收到 B 的消息后又通过 NAT 技术把 A 映射的某公网地址替换为 A 的内网地址并将数据转发给主机 A。