网安期末提纲

1、端口号于是对应的协议（P28）考试不考

2、网络攻防技术（下面各有各的详解，这里先记有哪几种）

2.1、攻击：（P9）

2.2、防御：（P10）

3、网络信息安全分类（P2-3）

3.1、物理安全

3.2逻辑安全（下面四点是我概括的，最好看书自己概括）

4、缓冲区溢出攻击（P78）

4.1定义：缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖...

4.2几种容易造成缓冲区溢出的c语言函数以及对应替代函数

4.3、如何防御？P84

5、SQL注入攻击和XSS跨站脚本攻击

5.1、SQL注入（p92）：

5.2、XSS（p106，第一段第二段总结）

6、防火墙（p121）

6.1、分类（技术）

6.2、三个接口

6.3、安全策略：No-规则型，Yes-规则型

6.4、基本功能

6.5、特性

6.6、局限性

6.7、体系结构

6.7.1、分组过滤路由器

6.7.2、双宿主机

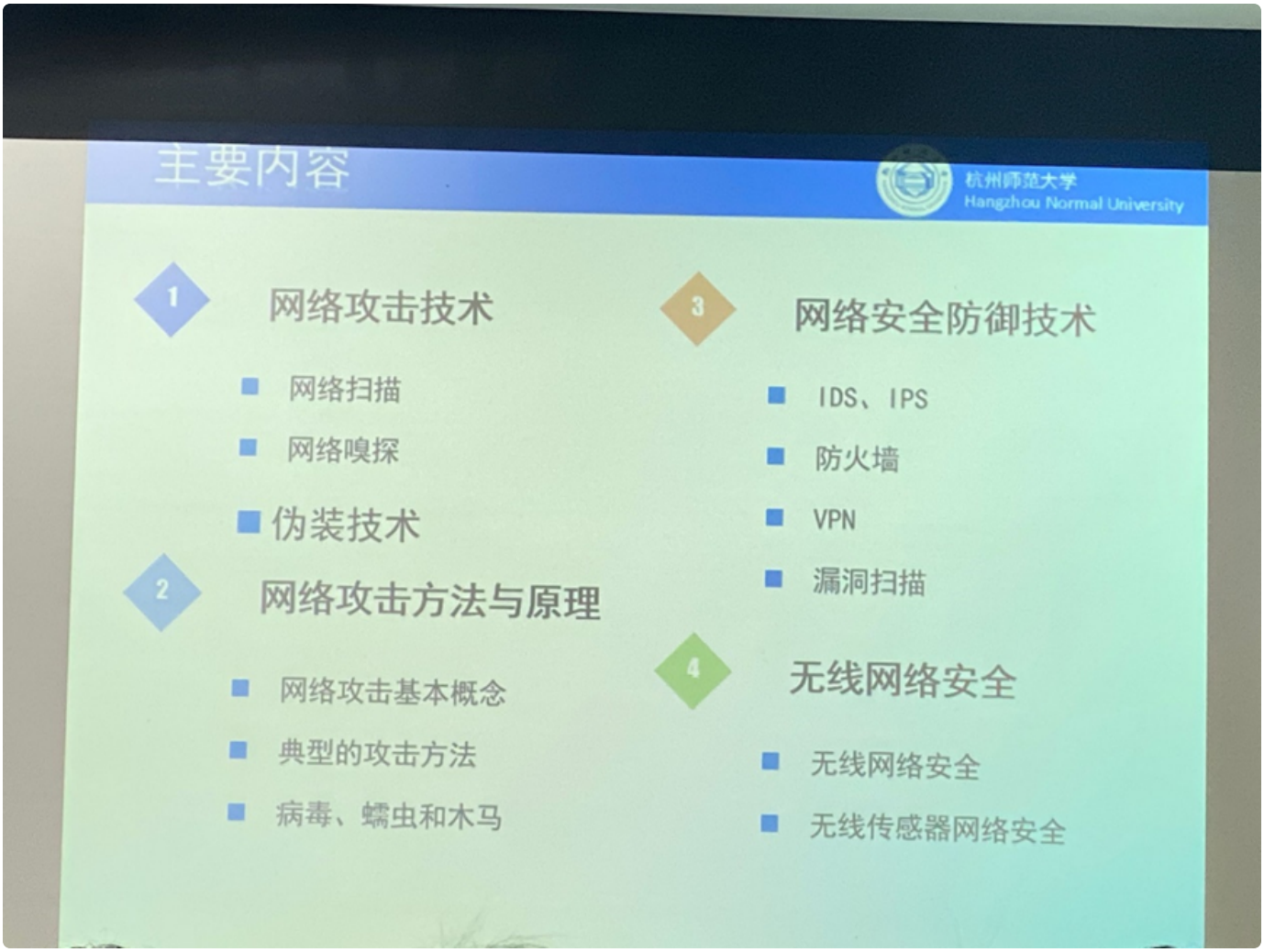
6.7.3、屏蔽主机

6.7.4、屏蔽子网

7、VPN（虚拟专用网络）

7.1、安全技术：

考点：



1、端口号于是对应的协议（P28）考试不考

端口号	协议
21	FTTP（文件传输协议）
23	Telnet（远程终端协议）
25	SMTP（简单邮件传输协议）
53	DNS（域名解析协议）
80	HTTP（超文本传输协议）
139	NETBIOS会话服务端口
443	HTTPS（超文本传输安全协议）
445	RPC协议（远程调用协议）
–	ARP协议
3389	远程桌面的服务端口，用到很多协议

2、网络攻防技术（下面各有各的详解，这里先记有哪几种）

2.1、攻击：（P9）

（1）扫描
（2）嗅探
（3）伪装

2.2、防御：（P10）

（1）IDS，IPS
（2）防火墙
（3）VPN
（4）漏洞扫描

3、网络信息安全分类（P2–3）

3.1、物理安全

保护计算机硬件和存储介质的装置和工作程序。

3.2逻辑安全（下面四点是我概括的，最好看书自己概括）

①限制登录次数，防止穷举攻击
②文件、图像、视频加密
③权限控制
④跟踪可疑的、未授权的存储企图
（3）操作系统安全
多人使用计算机时，保证操作系统能区分用户，防止他们互相干扰。
（4）网络数据传输安全
保护数据在网络信息系统中传输、交换和存储的保密性、完整性、真实性、可靠性、可用性和不抵赖性等。

4、缓冲区溢出攻击（P78）

4.1定义：缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖在相邻内存区域的数据上（即覆盖合法数据）。

4.2几种容易造成缓冲区溢出的c语言函数以及对应替代函数

容易缓冲区溢出的函数	替代函数
strcpy()	strncpy()
strcat()	strncat()
gets()	fgets()
sprintf()、vsprintf()	采用指定长度，如 springf(usage,”%s\n”,BUF_SIZE,argv[0])
scanf系列 sscanf()、fscanf()、vfscanf()、vscanf()、vsscanf()	设置宽度
strdup()	strndup()，字符串复制
getchar()、fgetc()、getc()、read()	循环中使用建议检查缓冲区边界

4.3、如何防御？P84

- 强制写正确的代码的方法（上面的函数使用）
- 基于探测方法的防御
    - 基于源代码的静态检测技术

    - 基于目标代码的检测技术
    - 基于源代码的动态检测技术
- 基于操作系统底层的防御
    - 库函数的保护
    - 操作系统内核补丁保护

5、SQL注入攻击和XSS跨站脚本攻击

5.1、SQL注入（p92）：

攻击服务器端，主动攻击（黑客直接攻击服务器）
特点：①隐蔽性强，②广泛性，③易学，④危害性大
分类：常规注入，字典注入，盲注

5.2、XSS（p106，第一段第二段总结）

攻击者攻击客户端，如用户浏览的html网页，嵌入web的代码会被执行（被动攻击，用户不访问这个网页就不会受到攻击）
分类：反射型，存储型和DOM型
P106第一段第二段总结（重点☆☆☆☆☆）
从原理上讲，XSS攻击与SQL注入攻击是一样的，即因程序对用户输入的数据没有过滤造成的，攻击发生的场景在客户端，攻击的载体在用户的客户端浏览器上，XSS攻击是一种被动攻击。
攻击者将恶意数据上传到Web服务器上，若应用程序没有将这些内容进行检测过滤，就使这些恶意代码逻辑包含在服务器动态产生或更新的网页中。当客户端程序对相应内容进行解释时，恶意数据就具有了文本之外的特殊含义，它可能会执行一系列具有危害性质的代码，从而使访问该网页的用户受到攻击。攻击者可以做很多让人意想不到的事情，如果浏览器或浏览器控件的漏洞导致脚本能够读取、写入甚至执行用户硬盘的文件，结果不堪设想。

6、防火墙（p121）

6.1、分类（技术）

- 包过滤（粒子检测）
- 状态检测
- 应用代理（p122）
- 网络地址转换NAT（笔记记了）

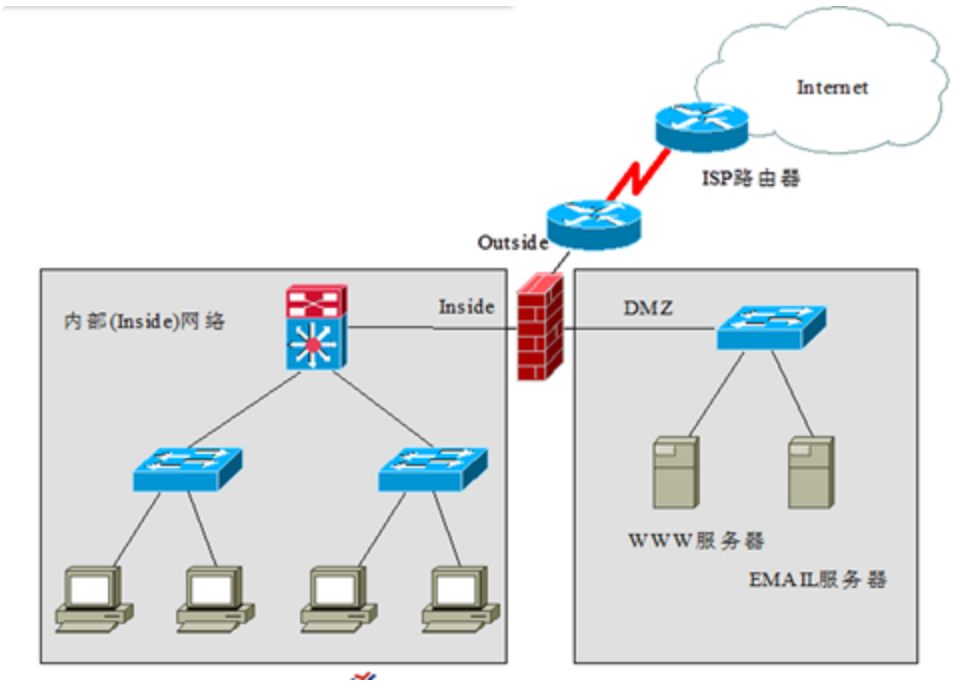
以上防火墙优缺点的比较如表 9-1 所示。

表 9-1　各类防火墙的优缺点比较

类型性能	综合安全性	网络层保护	应用层保护	应用层透明	整体性能	处理对象
简单包过滤型防火墙	★	★★★	★	★★★★★	★★★★	单个数据包报头
状态检测包过滤防火墙	★★	★★★★	★★	★★★★★	★★★★★	单个数据包报头一次会话
应用代理型防火墙	★★★	★	★★★★	★	★	单个数据包数据
复合型防火墙	★★★★	★★★★★	★★★★★	★★★	★★	单个数据包全部数据
核检测防火墙	★★★★	★★★★★	★★★★★	★★★★	★★★★★	一次完整回话应用数据

6.2、三个接口

- 外部网络（外网）：Internet
- 内部网络（内网）：Intranet
- 停火区（DMZ，非军事化区）



6.3、安全策略：No-规则型，Yes-规则型

6.4、基本功能

- 网络安全的屏障

- 强化安全策略
- 对网络存取和访问进行监控审计
- 防止内部信息的外泄
- 安全策略的检查
- 实施VPN和NAT的理想平台

6.5、特性

- 所有内部和外部之间的数据传输都经过防火墙；
- 只有合法数据（防火墙规则允许的数据）才能通过防火墙；
- 防火墙本身具有防入侵功能，不受各种攻击的影响；
- 防火墙能有效地记录Internet上的活动；
- 防火墙能强化安全策略。

6.6、局限性

- 不能防范恶意的内部用户的恶意破坏；
- 不能防范不通过防火墙的连接；
- 不能防止感染了病毒的软件或文件传输；
- 不能防范IP地址欺骗；入侵者可以绕过防火墙，找到防火墙中可能开启的后门；
- 人为因素在很大程度上影响其功能。

6.7、体系结构

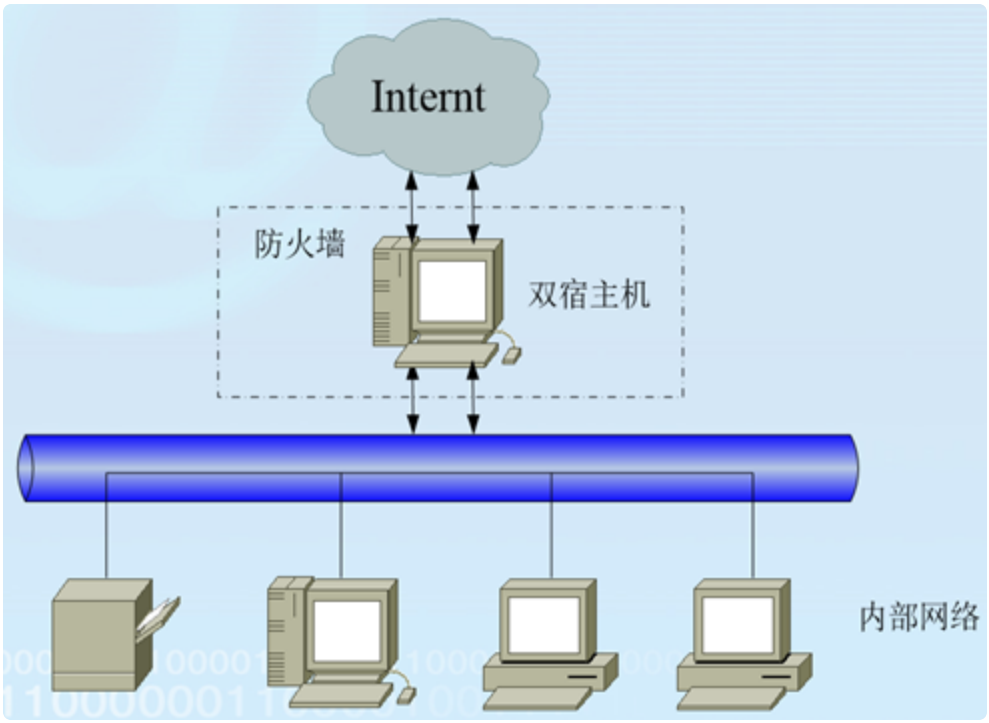
6.7.1、分组过滤路由器

作为内外网连接的唯一通道，要求所有的报文都必须在此通过检查。通过在分组过滤路由器上安装基于IP层的报文过滤软件，就可利用过滤规则实现报文过滤功能

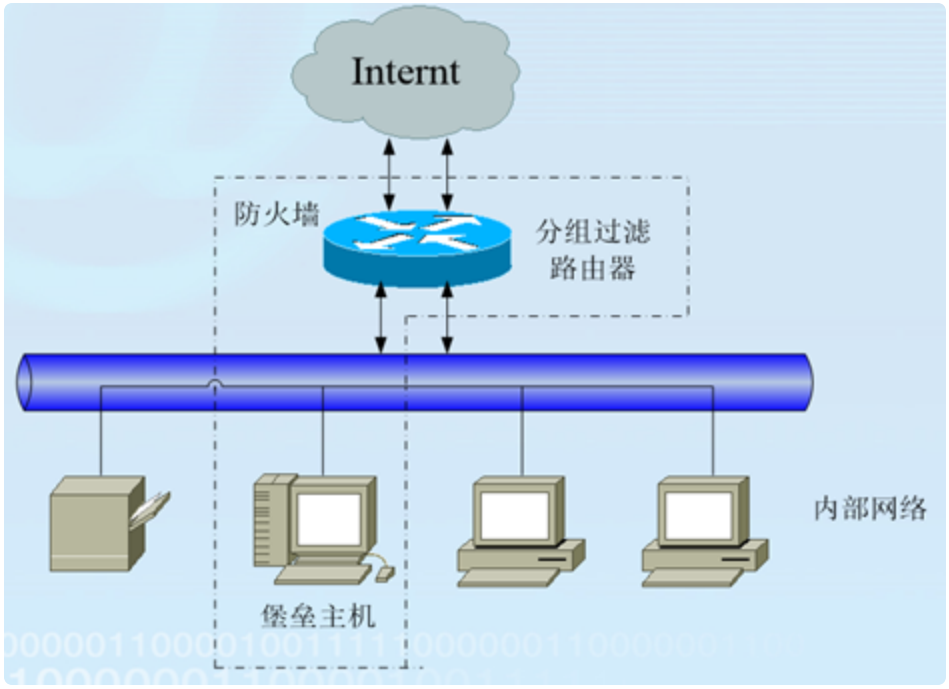
6.7.2、双宿主机

代理服务，堡垒主机上运行着防火墙软件，可以转发应用程序和提供服务等
优缺点：

- 堡垒主机的系统软件可用于身份认证和维护系统日志，有利于进行安全审计
- 该方式的防火墙仍是网络的“单失效点”。
- 隔离了一切内部网与Internet的直接连接，不适合于一些高灵活性要求的场合

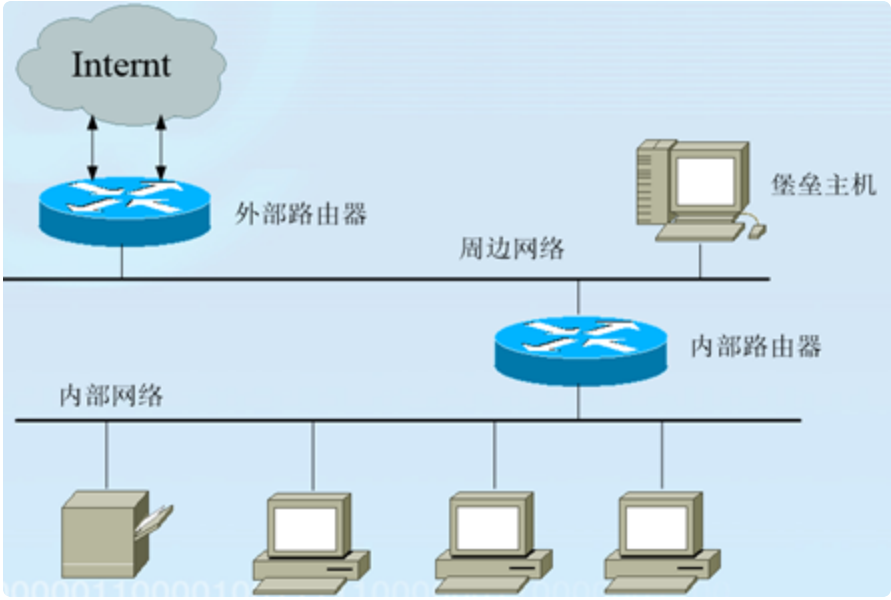


6.7.3、屏蔽主机



6.7.4、屏蔽子网

是最安全的防火墙系统，它在内部网络和外部网络之间建立一个被隔离的子网（非军事化区，DMZ）



7、VPN（虚拟专用网络）

7.1、安全技术：

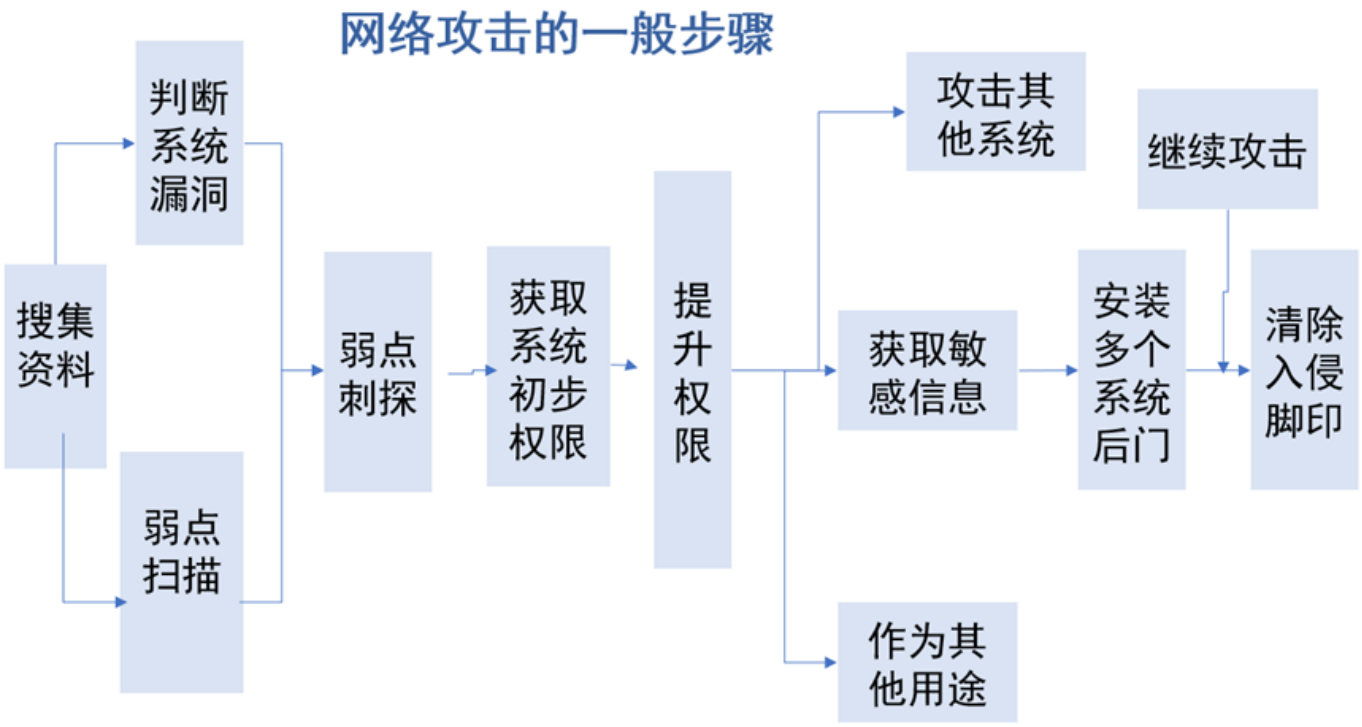
- 加密：加解密技术，秘钥管理技术
- 身份认证：用户名、密码、智能卡等
- 隧道封装：隧道协议将其它协议的数据包重新封装在新的包头中发送

7.2、VPN优点

- 可以快速构建网络，减小布署周期
- 与私有网络一样提供安全性，可靠性和可管理性
- 可利用Internet，无处不连通，处处可接入
- 简化用户侧的配置和维护工作
- 提高基础资源利用率
- 客户可节约使用开销
- 对于运营商可以有效利用基础设施，提供大量、多种业务

8、蜜罐技术（笔记没记，去ppt上看）

9、网络攻击的步骤



A：黑客

B：肉机

C：模拟机

D：被攻击者

攻击步骤：A通过B试探（漏洞扫描和弱点刺探）D，然后用C模拟D的操作环境，在C中进行获取权限、提升权限等攻击操作，练习完成后攻击D，然后安装后门，继续攻击，攻击完后清除脚印。

10、一些重要的实验操作命令行

10.1、控制他人电脑的C盘作为自己的K盘

net use k: \被攻击对象的ip地址\c$

10.2、创建用户AAA

net user AAA 123 /add

给用户AAA提权

net localgroup administrators AAA /add

10.3、自动关机

shutdown –s –t 180 –c "welcome"

10.4、死亡之ping

ping –t –1 65530 攻击对象的ip地址

11、DoS攻击（拒绝服务攻击，属于阻塞类攻击）

攻击网络协议权限或耗尽被攻击对象的资源，即破坏网络服务的一种技术方式。

11.1、ICMP泛洪

以所攻击的主机地址作为源地址，广播地址为目的地址发送一个ICMP ECHO请求包时，其它主机进行应答时，应答包会被发送到所攻击的主机上

11.2、Smurf攻击

攻击者将ICMP ECHO的源地址设置为一个广播地址或某一子网的IP地址，目标主机以广播形式回复ICMP ECHO REPLAY，形成广播风暴。

11.3、LAND攻击

将目标的源地址和目标地址都设置成同一个地址，导致服务器建立空连接，直到超时

12、DDoS攻击（分布式拒绝服务攻击）

基于DoS的一种特殊形式，攻击者将多台受控制的计算机联合起来向目标计算机发动DoS攻击。TCP3次握手。

13、常见的网络攻击手段

- 阻塞类攻击：DoS，DDoS
- 控制类攻击：口令攻击，特洛伊木马，缓冲区溢出攻击
- 探测类攻击：扫描技术、体系结构刺探、系统信息服务收集
- 欺骗类攻击：IP欺骗和假消息欺骗（两者主要包括ARP欺骗、电子邮件欺骗、钓鱼欺骗、非技术类欺骗、web欺骗）
- 漏洞类攻击：针对扫描器发现的网络系统的各种漏洞实施的相应攻击
- 破坏类攻击：破坏类攻击指对目标机器的各种数据与软件实施破坏的一类攻击，包括计算机病毒、逻辑炸弹等攻击手段

14、病毒、蠕虫和木马

	特征	是否能自我复制	特点
病毒	1、非授权 2、执行性 3、隐蔽性 4、传染性 5、潜伏性 6、破坏性 7、可触发性	可以复制，病毒代码的明确目的是自我复制	与蠕虫相比，病毒可以破坏计算机硬件、软件和数据
蠕虫	病毒的子类，消耗内存或网络带宽，导致计算机停止响应。	可以自我复制	可以潜入用户的系统并允许其他用户或程序远程操控由蠕虫感染的计算机；不使用驻留文件即可在系统间复制自身，而病毒需要传播受感染的驻留文件
木马	表面有用实际有破坏作用的程序。可以创建进程	不可以自我复制	主要由电子邮件和文件下载传播。使木马传播，必须在计算机上有效地启动这些程序

15、几种欺骗类攻击

- IP地址欺骗

IP欺骗技术就是通过伪造某台主机的IP地址骗取特权从而进行攻击的技术。

危害：冒充互信主机组中的主机进行访问；可以使被信主机丧失工作能力

- ARP欺骗攻击

ARP欺骗攻击就是利用ARP协议漏洞，通过伪造IP地址和MAC地址实现ARP欺骗的攻击技术。

- DNS欺骗攻击

攻击者采用种种欺骗手段，使用户查询DNS服务器进行域名解析时获得一个错误的地址结果，从而可将用户引导到错误的互联网站点，或者发送一个电子邮件到一个未经授权的邮件服务器等。

- 源路由欺骗攻击

通过指定路由，以假冒身份与其他主机进行合法通信或发送假文，使受攻击主机出现错误动作 。

- 网络钓鱼(Phishing)是近几年新兴的一种攻击方式。“Phishing”一词由“Fishing”和“Phone”组合而来。由于黑客起初是以电话作案，所以用“Ph”来取代“F”，创造了“Phishing”，同时有“愿者上钩”之意。网络钓鱼通常采用发送大量欺骗性垃圾电子邮件和伪造Web站点等来进行诈骗活动。

16、ARP

16.1、定义

地址解析协议（ARP）是将IP地址映射成物理地址（网卡MAC地址）的一个TCP/IP。

16.2、网卡的4种接收模式

- 广播方式：设置该模式的网卡能接收网络中的广播信息
- 组播方式：设置该模式的网卡能接收组播信息
- 直接方式：只有目的网卡能接收到该数据
- 混杂模式：设置该模式的网卡能接收一切通过它的数据，不管该数据是否传给它

17、APT

17.1、定义

高级持续性威胁。是指组织(特别是政府)或者小团体利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式

17.2、特点：

- 隐蔽性强
- 潜伏期长，持续性强
- 目标性强

17.3、主要攻击手段

- 漏洞攻击
- 水坑攻击
- 鱼叉攻击

18、认证

18.1、提出

- 身份认证：身份欺诈，防止身份伪造
- 消息认证：防止消息伪造和篡改

18.2、需求

某一成员（声称者）提交一个主体的身份并声称它是那个主体

18.3、定义：

- 认证就是确认实体（或消息）是它所声明的。
- 身份认证对发送者的身份真假加以鉴别，防止身份假冒、欺骗
- 消息认证对发送消息的内容的完整性进行鉴别

18.4、认证技术

认证函数：

- H(M)，哈希函数，完整性确认
- H(M,KAB)对称秘钥<==>MAC
- H(pwd,salt)，双因子认证，基于口令加密

数字签名

生物特征认证

- 虹膜识别
- 面部识别
- 声音识别
- 指纹识别

认证方式	优点	缺点
口令认证 （此处为弱密码登录的认证方式）	①最简单也是最常用的认证方式 ②简单易用，易于操作	①记忆成本高，尤其是用户提取目标密码时试错成本偏高 ②存在撞库风险 ③不安全的认证方式，比如密码记不住记在别的地方被坏人发现进而造成损失；或是弱密码被穷举攻破
生物认证	①随身性 ②安全性 ③唯一性 ④稳定性 ⑤广泛性 ⑥方便性 ⑦可采集性	①外界环境或使用者本体会影响精确性 ②很多技术还没经过测试 ③很多认证用到激光，影响健康

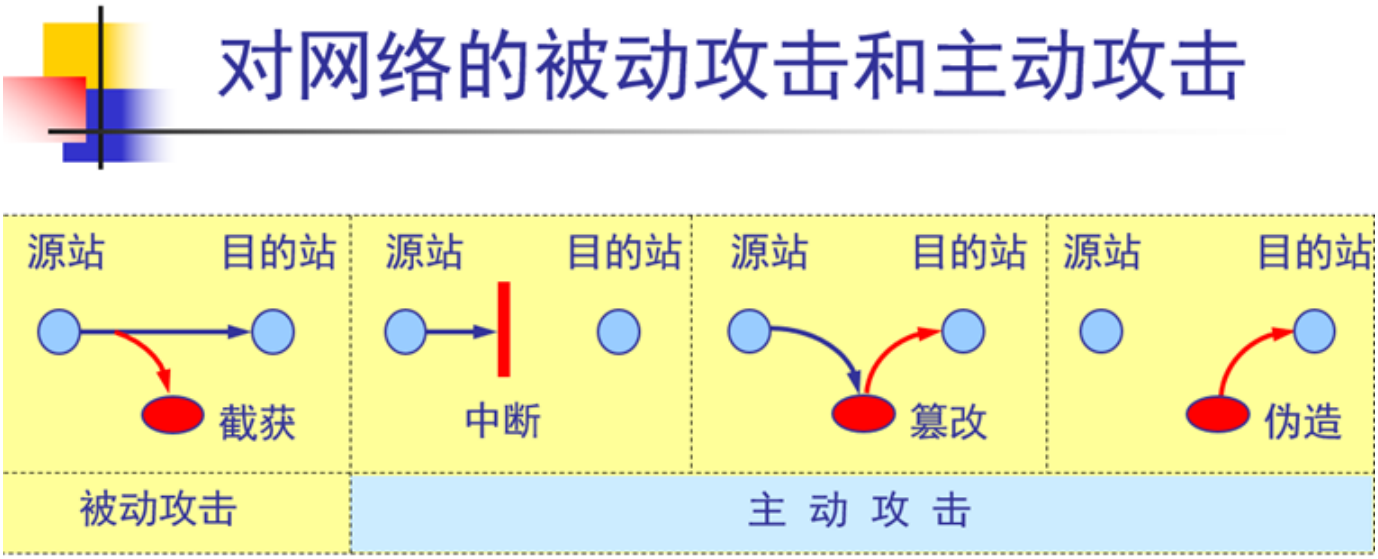
19、主动攻击和被动攻击

19.1、被动攻击

截获，指窃听到他人的通信内容

19.2、主动攻击：

- 中断：有意中断他人通信
- 篡改：故意篡改报文
- 伪造：伪造信息在网络上传送



20、IDS，IPS

20.1、IDS（入侵检测系统）：门卫！

特点：

- 实时性
- 可扩展性
- 适应性
- 安全性
- 有效性

作用

入侵检测

报警①误报：好人当坏人②漏报：坏人当好人

20.2、IPS（入侵防御系统）：

作用：阻止拦截

不但能检测入侵的发生，而且能通过一定的响应方式，实时地中止入侵行为的发生和发展，实时地保护系统不受实质性的攻击。

防火墙可以检测20%的攻击

IDS可以检测80%的攻击

IPS可以检测50%的攻击

21、堆溢出攻击五种攻击

- 内存变量
- 代码逻辑
- 函数返回地址
- 异常处理机制
- 函数指针