**self-defending network自防预网络**

**攻击和命中**

**攻击分为三类：(也可以说是三个步骤)**

**1、Reconnaissance 扫描探测攻击**

**2、Access attacks 访问攻击**

**3、Dos and distributed Dos 拒绝服务攻击**

**Reconnaissance扫描探测攻击**

**扫描探测攻击也叫侦查，是对系统、服务或弱点的非授权的发现与映射。是一种信息收集行为。**

**攻击的四种方法：**

**---Packet sniffers抓包**

**---Port scans端口扫描**

**---Ping sweeps (Ping扫描)**

**---Internet information queries 互连网查询**

**如何防止packet sniffers**

**---authentication 认证，使用一次性密码**

**---cryptography 加密，让你抓到包也看不了**

**---antisniffer tools 反抓包工具**

**---switched infrastructure 使用交换机，可以在端口上做阻止未知单、组播的泛洪**

**在交换机上防止被抓包的方法**

**switchport protect 隔离二层的通信，使二层的广播无法传播**

**switchport port-security 这条命令可用来限定一个端口只能学一个MAC地址，IE中考到哦**

**port scans和ping sweeps可以知道你主机使用的服务、端口、操作系统、漏洞**

**如何防止端口扫描**

**---尽量关闭无用服务**

**Access attacks访问攻击**

**---retrieve data**

**---gain access**

**---escalate their**

**Access attacks include:**

* **Password attacks 密码攻击**
* **Trust exploitation 信任利用或叫信任的拓展**
* **Port redirection 端口重定向**
* **Man-in-the-middle attacks 中间人攻击**
* **Buffer overflow 缓存溢出**

**Dos and distributed Dos 拒绝服务攻击**

**通常还会伴随地址欺骗，DOS攻击有很多种形式，但根本上它们都是通过耗尽系统资源来阻止已被授权的用户使用服务。**

**DOS**

**1、网络DOS**

**icmp smurf**

**udp echo fragle**

**2、主机DOS**

**3、ping of death ip 65536**

**4、rate-limit**

**防预DOS攻击的两大办法：**

**1、ios FW（防火墙）也就是CBAC**

**2、ip tcp intercept**

**DDOS分布式拒绝服务攻击**

**DDOS攻击是指用伪造的数据充满整个网络链路，这种数据能够淹没网络链接，导致合法的流量被丢弃。**

**ddos guard**

**-----------------------------------------------------------------------------------------**

**病毒、蠕虫、木马**

**防止worm蠕虫**

**---contain**

**---inoculate**

**---quarantine**

**---treat**

**Application layer attacks应用层攻击**

**通过使用IDS/IPS来进行预防**

**禁用路由器上一些不必要的服务和端口来降低被攻击的可能性：**

**在IOS12.4之后--auto secure命令可以自动关闭不必要的接口和服务**

**ip finger**

**connected 10.1.1.1 finger 这个服务可以看到对端路由器上有哪些用户**

**telnet 10.1.1.1 finger**

**telnet 10.1.1.1 echo**

**telnet 10.1.1.1 discard**

**telnet 10.1.1.1 daytime**

**telnet 10.1.1.1 chargen**

**clock tinezone GMT +8 设置时区**

**NTP**

**NTP的server提供时钟源，client端同步**

**R1(config)#ntp master 让本台路由器做为server端发送时钟**

**R2(config)#ntp server 150.100.1.1 和地址为150.100.1.1的server端同步时钟**

**注意：只同步时钟，不会同步时区**

**router(config)#clock timezone GMT +8 配置时区的命令**

**R2(config)#ntp authentication-key 1 md5 cisco**

**R2(config)#ntp trusted-key 1**

**R2(config)#ntp authenticate**